НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Інформаційно-телекомунікаційних мереж

«На правах рукопису»

УДК _____

«До захисту допущено»

Завідувач кафедри

_____ Лариса ГЛОБА

«___»_____2020 р.

Магістерська дисертація

на здобуття ступеня магістра
за освітньо-професійною програмою «Інформаційно-комунікаційні технології»
зі спеціальності 172 «Телекомунікації та радіотехніка»

на тему: «Вдосконалений метод оцінки рівня безпеки абонентського з'єднання при організації віддаленого доступу»

Виконав:
студент VI курсу, групи ТІ-91мп
Пилипчук Ангеліна Олександрівна _____

Керівник:
доцент кафедри ІТМ ІТС, доцент, к.т.н.
Правило Валерій Володимирович _____

Рецензент:
доцент кафедри ТК ІТС, доцент, к.т.н.
Явіся Валерій Сергійович _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Інформаційно-телекомунікаційних мереж

Рівень вищої освіти – другий (магістерський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інформаційно-комунікаційні технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Лариса ГЛОБА
«___»_____2020 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Пилипчук Ангеліні Олександрівні

1. Тема дисертації «Вдосконалений метод оцінки рівня безпеки абонентського з'єднання при організації віддаленого доступу», науковий керівник дисертації доцент кафедри інформаційно-телекомунікаційних мереж ІТС Правило Валерій Володимирович, доцент, к.т.н.,, затверджені наказом по університету від «03» листопада 2020 р. № 3208-с

2. Термін подання студентом дисертації 10.12.2020 р.

3. Об'єкт дослідження: процес забезпечення безпечної передачі даних при віддаленому доступі до мережних ресурсів.

4. Предмет дослідження: метод оцінки рівня безпеки абонентського з'єднання при організації віддаленого доступу.

5. Перелік завдань, які потрібно розробити:
   1. дослідити методи безпеки та конфіденційності при віддаленому доступі;

2. провести аналіз можливих заходів для забезпечення безпеки при віддаленому доступі;
3. дослідити сучасні та потенційні джерела та проблемні операції MFA
4. запропонувати вдосконалений метод оцінки рівня безпеки абонентського з'єднання.

6. Орієнтовний перелік ілюстративного матеріалу

7. Орієнтовний перелік публікацій

1. Перспективи телекомунікацій 2019 – Прискорення алгоритмів шифрування реалізованих на основі графічних процесорів, Пилипчук А. О.Правило В.В.
2. Перспекиви розвитку інформаційно-телекомунікаційних технологій та систем 2019 – Використання технології Cuda для прискорення алгоритму шифрування.
3. Перспективи телекомунікацій 2020 – Моделі ідентифікації та аутентифікації в системах хмарних вичислень для веб-серверів та мобільних додатків з інтелектуальною підтримкою вибору, Пилипчук А. О.

8. Дата видачі завдання 01.09.2019 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Проведення огляду систем віддаленого доступу.	01.01.2020	виконано
2	Дослідження методів безпеки та конфіденційності.	01.03.2020	виконано
3	Дослідження технології VPN.	05.05.2020	виконано
4	Проведення аналізу можливих заходів для забезпечення безпеки.	01.06.2020	виконано
5	Аналіз багатофакторної автентифікації.	10.06.2020	виконано
6	Дослідження сучасних та потенційних джерел MFA.	01.08.2020	виконано
7	Дослідження проблеми операції MFA.	09.09.2020	виконано
8	Опис вдосконаленого методу оцінки рівня безпеки абонентського з'єднання.	02.10.2020	виконано
9	Розробка стартап-проекту моделювання	08.11.2020	виконано
10	Підготовка звітної документації.	10.12.2020	виконано

Студент Ангеліна ПИЛИПЧУК

Науковий керівник дисертації Валерій ПРАВИЛО

РЕФЕРАТ

Робота містить 107 сторінок, 15 рисунків 21 таблиць. Було використано 41 джерел.

Актуальність теми:

Актуальність теми обумовлена зростанням цінності інформації, постійною появою нових загроз інформаційної безпеки та важливістю процесу автентифікації при побудові захисту інформаційної системи. На даний момент не існує універсального рішення, яке може забезпечити необхідний рівень захищеності автентифікації в будь-якій розподіленій системі. Багато широко поширені в даний час алгоритми автентифікації залишаються уразливими для різних типів атак. У той же час алгоритми, що володіють достатнім ступенем захищеності, зазвичай вимагають наявності складної інфраструктури і залишаються незрозумілими для широкого кола користувачів.

Запропоноване рішення багатофакторної автентифікації охоплює випадки автентифікації користувача, навіть якщо деякі з факторів не збігаються або відсутні. Це також допомагає кваліфікувати відсутні чинники, не розкриваючи конфіденційні дані перевертючої сторони.

Мета дослідження:

Ця робота спрямовано на підвищення рівня безпеки абонентського з’єднання за рахунок забезпечення гнучкості роботи багатофакторної автентифікації для встановлення безпечного зв'язку між користувачем і віддаленим сервером.

Задачі дослідження:

1. дослідити методи безпеки та конфіденційності при віддаленому доступі;

2. провести аналіз можливих заходів для забезпечення безпеки при віддаленому доступі;
3. дослідити сучасні та потенційні джерела та проблемні операції MFA;
4. запропонувати вдосконалений метод оцінки рівня безпеки абонентського з’єднання.

Об’єкт дослідження: процес забезпечення безпечної передачі даних при віддаленому доступі до мережних ресурсів.

Предмет дослідження: метод оцінки рівня безпеки абонентського з’єднання при організації віддаленого доступу.

Методи дослідження: основними методами дослідження є математичне та імітаційне моделювання.

Наукова новизна:

Запропоновано новий метод оцінки рівня безпеки абонентського з’єднання при організації віддаленого доступу, що забезпечує заданий рівень безпеки за рахунок гнучкості роботи багатофакторної автентифікації.

Запропоноване рішення багатофакторної автентифікації охоплює випадки автентифікації користувача, навіть якщо деякі з факторів не збігаються або відсутні.

Практичне значення одержаних результатів:

Застосування метода оцінки рівня безпеки абонентського з’єднання при організації віддаленого доступу.

Публікації:

Результати магістерської дисертації опубліковано у 3 збірних матеріалів конференцій.

Ключові слова: віддалений доступ, автентифікація, захист інформації, VPN, SFA, 2FA, MFA

ABSTRACT

The work contains 107 pages, 15 figures and 21 tables. 41 sources were used.

Relevance of the topic:

The relevance of the topic is due to the growing value of information, the constant emergence of new threats to information security and the importance of the authentication process in building the protection of the information system. There is currently no one-size-fits-all solution that can provide the required level of authentication security in any distributed system. Many currently common authentication algorithms remain vulnerable to different types of attacks. At the same time, algorithms with a sufficient degree of security usually require a complex infrastructure and remain incomprehensible to a wide range of users.

The proposed multifactor authentication solution covers instances of user authentication, even if some of the factors do not match or are missing. It also helps to classify the missing factors without disclosing the confidential data of the verifying party.

Research objectives:

1. explore security and privacy methods for remote access;
2. to analyze possible measures to ensure security in remote access;
3. explore current and potential sources and problematic MFA operations;
4. to offer an improved method of assessing the security level of the subscriber connection.

Object of research: the process of ensuring secure data transmission with remote access to network resources.

Subject of research: method of assessing the level of security of the subscriber connection when organizing remote access.

Methods of research: the main methods of research are mathematical modeling and simulation.

Scientific novelty of the obtained results:

A new method for assessing the security level of a subscriber connection when organizing remote access is proposed, which provides a given level of security due to the flexibility of multifactor authentication.

The proposed multifactor authentication solution covers instances of user authentication, even if some of the factors do not match or are missing.

The practical value of the results obtained:

Apply the method of assessing the security level of the subscriber connection when organizing remote access.

Publications:

The results of the master's dissertation are published in 3 conference proceedings.

Keywords: remote access, authentication, information security, VPN, SFA, 2FA, MFA.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

FTP	File Transfer Protocol	Протокол передачі файлів в мережі
HTTP	HyperText Transfer Protocol	Протокол передачі гіпер-текстових документів
IKE	Internet Key Exchange	Стандартний протокол набору протоколів IPsec
IP	Internet Protocol	Інтернет протокол
IPsec	IP Security	Набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу IP
MFA	Multi-Factor Authentication	Багатофакторна автентифікація
PPP	Point-to-Point Protocol	Протокол точка-точка
PPTP	Point-to-Point Tunneling Protocol	Тунельний протокол типу точка-точка
SFA	Single-Factor Authentication	Однофакторна автентифікація
SLIP	Serial Line Internet Protocol	Протокол Інтернет для послідовної лінії
SSL	Secure Sockets Layer	Рівень захищеності сокетів
TCP	Transmission Control Protocol	Протокол керування передаванням

TLS	Transport layer security	Захист на транспортному рівні
PIN	Personal Identification Number	Персональний ідентифікаційний номер
ID	Identification Number	Identification Number
ECG	Electrocardiography	Електрокардіографія
GPS	Global Positioning System	Система глобального позиціонування
FTE	Failure to Enroll	Помилка реєстрації
FTA	Failure to Acquire	Неможливість придбання
CER	Crossover Error Rate EER	Похибка кросовера EER
EER	Equal Error Rate	Рівний рівень помилок
FAR	False Accept Rate	Помилковий коефіцієнт прийняття
VPN	Virtual Private Networks	Віртуальна приватна мережа

ВСТУП

В даний час офіси втрачають чіткі межі. В організаціях комп’ютерна мережа не обмежується лише локальною мережею, яка розміщена в одному чи в декількох офісах, що близько розташовані між собою. Мобільність набирає велику популярність. Користувачі тепер можуть знаходитись на великій відстані від головного офісу, наприклад, якщо філії знаходяться в інших містах чи країнах або коли працівник організації їде у відрядження.

Цю проблему можна вирішити організувавши віддалений доступ. Для організації віддаленого доступу можуть використовуватися різні схеми і продукти. Продукти віддаленого доступу можуть істотно відрізнятися реалізованими в них функціями, а значить, і можливостями при вирішенні конкретної практичної задачі.

Не дивлячись на всі переваги віддаленого доступу виникає ряд проблем, що можуть завадити. Причиною тому множинні обмеження. Першим обмеженням є вимога до швидкості інтернет-з'єднання, оскільки мала швидкість стає причиною спотворень в зображенні, звуках і т.д. При відкритті віддаленого доступу ви піддаєте свій ПК деякої небезпеки, оскільки, фактично, «викладаєте» всі матеріали в глобальну мережу, проте і це легко вирішується за допомогою грамотної конфігурації налаштувань програми.

У такому пов'язаному світі, механізм захисту захищених переданих даних - це, насамперед, автентифікація. Автентифікація залишається основним захистом від незаконного доступу до пристрою чи будь-якого іншого додатка, офлайн чи в режимі онлайн.

РОДІЛ 1
ОГЛЯД СИСТЕМ ВІДДАЛЕНОГО ДОСТУПУ

Віддалений доступ – це широке поняття, що об’єднує в собі різні варіанти взаємодії мереж, комп’ютерів та додатків. Існує багато схем взаємодії, які можливо віднести до віддаленого доступу. Для них характерне використання глобальних мереж чи глобальних каналів. Також, віддаленому доступу притаманна несиметричність взаємодії, коли, центральний комп’ютер чи центральна мережа з однієї сторони, а з іншої - окремий комп’ютер, термінал або маленька мережа, яким потрібний доступ до ресурсів головної мережі.

Системи віддаленого доступу – технології, які надають прозоре підключення для віддалених користувачів, що розташовані не в локальній мережі компанії. Віддалений доступ найбільш використовують для підключення домашніх комп’ютерів, ноутбуків чи телефонів робітників до мережі організації. Провайдери інтернету також користуються віддаленим доступом, щоб підключати своїх клієнтів до мережі інтернет [1].

Коли клієнти запускають програми віддаленого доступу, вони ініціюють підключення до головного сервера. Потім сервер робить перевірку автентифікації та обслуговує зв’язок під час підключення, до тих пір коли сеанс не завершиться користувачем чи адміністратором мережі.

Для доступу до ресурсів користувачі віддаленого доступу використовують стандартні засоби. Наприклад, віддалений клієнт, що працює на комп’ютері з Windows, може підключитися до мережевого диску чи принтеру за допомогою провідника Windows. Підключення є постійним – це означає, що під час віддаленого сеансу користувачам не потрібно постійно підключатися до мережевих ресурсів. Так як при віддаленому доступі повністю підтримуються букви дисків та універсальні імена UNC (Uniform Naming Convention).

Більшість комерційних та користувацькі додатки працюють без додаткових модифікацій [1].

На Рис.1.1 представлений логічний еквівалент підключення віддаленого клієнта до сервера віддаленого доступу.

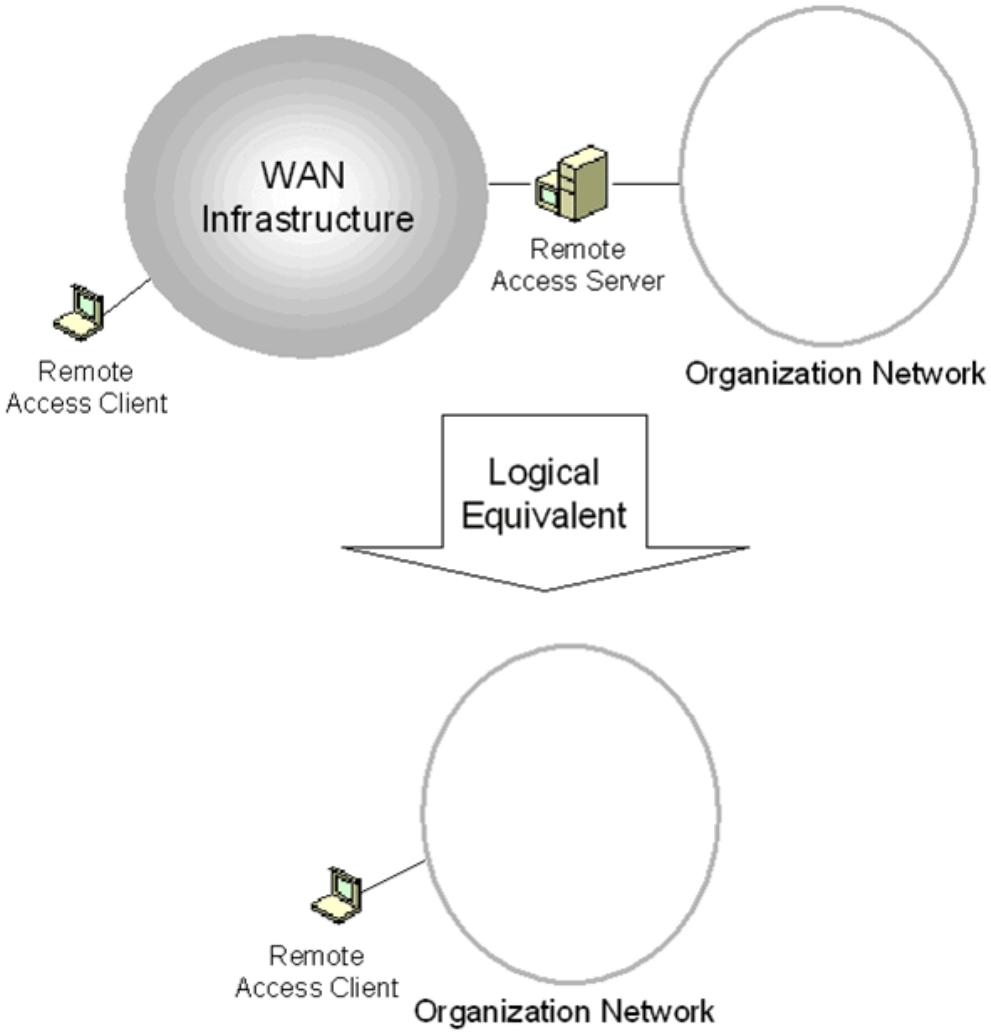


Рис.1.1 Логічний еквівалент підключення віддаленого доступу

Розрізняють два основних види віддаленого доступу:

- З’єднання по комутованій лінії (dial-upconnection);
- З’єднання з використанням віртуальних приватних мереж (Virtual Private Networks, VPN).

Обидва види з’єднань працюють за моделлю «клієнт-сервер». Клієнт віддаленого доступу – це комп’ютер, який має можливість підключатися до віддаленого комп'ютера і працювати з його ресурсами або з ресурсами віддаленої мережі однаково, як з ресурсами своєї місцевої мережі. Єдина відмінність віддаленої роботи від локальної з точки зору клієнта - більш низька швидкість з'єднання. Сервер віддаленого доступу (Remote Access Services, RAS) - це комп'ютер, здатний приймати вхідні запити від клієнтів віддаленого доступу і надавати їм власні ресурси або ресурси своєї локальної мережі.

Підключення віддаленого доступу, зображене на Рис.1.2, складається з клієнта віддаленого доступу, сервера віддаленого доступу та інфраструктури глобальної мережі (Wide Area Network, WAN).

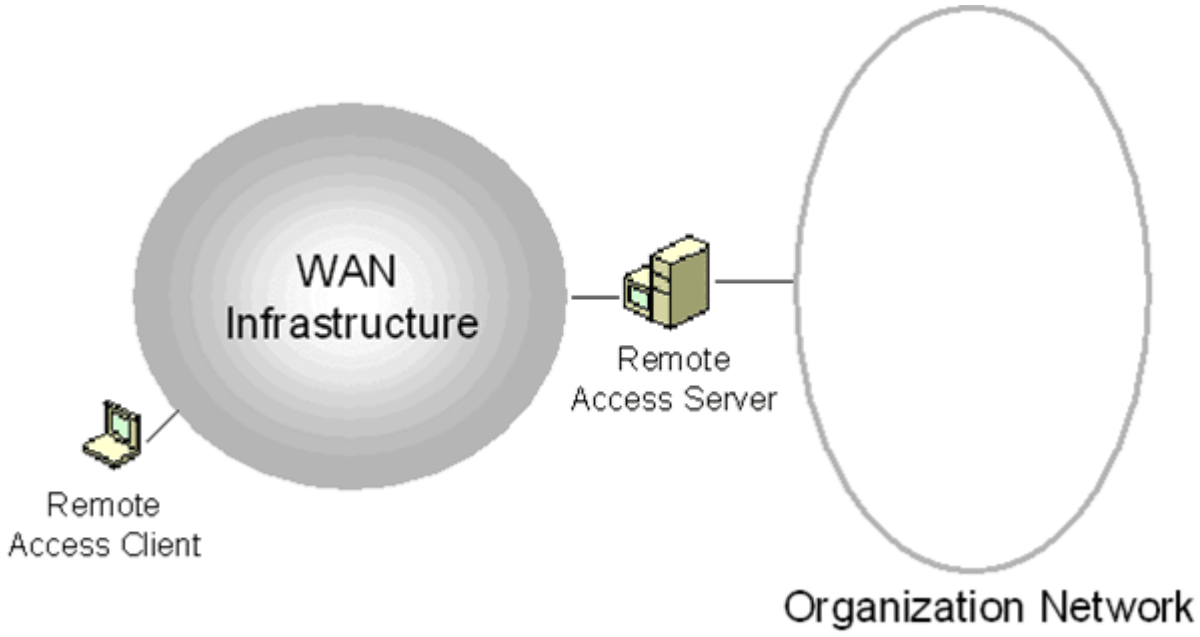


Рис.1.2 Компоненти підключення віддаленого доступу

1.1 Дослідження методів віддаленого доступу

Існує три методи підключення віддаленого користувача або відділення фірми до локальної мережі компанії:

• Емуляція термінала - це метод, при якому користувач віддаленого терміналу за допомогою спеціального програмного забезпечення підключається по глобальній мережі до іншого комп'ютера, як локальний вузол. Цей спосіб часто використовується на основному комплекті і міні-комп'ютерах, але мало поширений в локальній мережі.

• Віддалене керування – це метод, який дозволяє віддаленому користувачу керувати одним комп’ютером в локальній мережі.

• Метод віддаленого вузла заснований на використанні сервера віддаленого доступу, який дозволяє окремим комп’ютерам або локальним мережам з’являтись з центральною мережею. Програмне забезпечення віддаленого комп’ютера, що реалізує функції віддаленого вузла, дозволяє йому функціонувати як повноцінний користувач локальної мережі.

Аналіз методу термінального доступу

Принцип роботи термінального доступу працює так, що віддалений термінал не виконує обчислення. Всі процеси відбуваються на центральних машинах, інформація перенаправляється від клавіатури та миші терміналу. Після обробки графічна інформація передається на монітор терміналу.

Переваги системи термінального доступу:

• Відсутність в кінцевому обладнанні складних деталей і проведення модернізації на сервері замість клієнтських станцій збільшує термін служби терміналів до 7-10 років. Також істотно знижується рівень енергоспоживання всієї мережі (приблизно на дві третини, в порівнянні з мережею зі звичайних комп'ютерів).

• Установка ліцензій на сервері з урахуванням кількості одночасно працюючих в програмі користувачів, а не з урахуванням загальної кількості робочих місць, зменшує фінансові витрати на придбання відповідного

програмного забезпечення, оскільки, наприклад, замість 40 ліцензій купується лише 10.

- Відсутність знімних накопичувачів інформації робить неможливим будь-яке копіювання даних користувачем.
- Відсутність можливості самостійно встановлювати програми робить неможливим занесення користувачем вірусу в базу даних і запобігає виникненню конфлікту між різними додатками.
- Зберігання даних тільки на сервері зводить до мінімуму ризик втрати важливої інформації внаслідок збоїв в роботі кінцевого обладнання (на сервері всі дані автоматично копіюються і зберігаються окремо).
- Модернізація обладнання зачіпає тільки сервер, при цьому для користувача станції абсолютно не потребують додаткові налаштування.
- Адміністрування мережі максимально спрощено за рахунок централізованого управління всіма станціями через сервер. Для обладнання нового робочого місця досить підключення до мережі додаткового терміналу, налаштування якого займає менше години і не вимагає фізичної присутності IT-фахівця.

Недоліки системи термінального доступу:

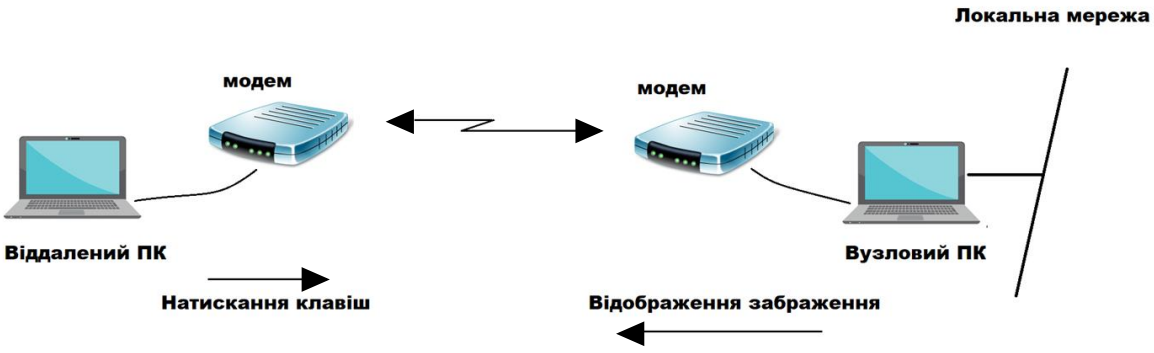
- Відсутність зв'язку між терміналом і сервером або поломка сервера робить неможливим продовження роботи всіх користувачів мережі.
- Помилки адміністратора при налаштуванні програмного забезпечення сервера тягнуть некоректну роботу всіх призначених для користувача робочих місць.
- При використанні деяких програмних продуктів (наприклад, від Microsoft) можуть знадобитися додаткові ліцензії - як на програмне

забезпечення, так і для роботи з самим термінальним сервером та іншим обладнанням, що спричиняє збільшення витрат на придбання ліцензій.

Використання термінального доступу в якості ефективного IT-рішення підходить, перш за все, для динамічної зростаючих організацій, де постійне збільшення кількості робочих місць вимагає більш раціонального використання наявних у компанії ресурсів [2].

Аналіз методу віддаленого керування

Віддалене керування – це метод, який дозволяє віддаленому користувачу отримати контроль над комп'ютером який знаходиться в локальній мережі корпорації. Швидкість проведення сеансу та його можливості залежать від характеристик керованого комп'ютера, тому що на ньому виконується обробка всіх мережевих команд. Коди натискання клавіш, які робляться на віддаленому комп'ютері, надсилаються на керований комп'ютер, а всі зміни транслюються на екран віддаленого пристрою. Файли та прикладні програми не завантажуються в віддалений комп'ютер. Недоліком методу є використання двох пристроїв для однієї роботи [3]. Принцип роботи віддаленого управління



показано на Рис.1.3.

Рис.1.3 Принцип роботи віддаленого управління

Для роботи на двох комп’ютерах: віддаленій системі та хост-системі, потрібне спеціальне програмне забезпечення для віддаленого керування. Система, що є віддаленою може бути ПК філіалів, домашнім ПК чи портативний комп’ютер, місцезнаходження якого змінюється щодня. Хост-системою може бути будь-який комп'ютер, підключений до локальної мережі, налаштований для віддаленого доступу.

За допомогою віддаленого управління мобільні працівники, які використовують ноутбуки або працівники філій, що використовують робочі станції, керують ПК у корпоративній мережі. Всі натискання клавіш користувача та переміщення миші відправляються на корпоративний комп'ютер, а зображення на цьому екрані пересилається на ноутбук для відображення. Це так, як якщо б користувач сидів перед комп'ютером, підключеним до мережі. Віддаленим користувачам не потрібні копії програм на своїх комп'ютерах, оскільки програми реально працюють на локальних робочих станціях у штаб-квартирі корпорації [4].

Метод віддаленого управління має ряд переваг:

- Це підвищує продуктивність додатків, які не потребують графічного інтерфейсу користувача. Ці програми зазвичай не призначені для архітектури клієнт / сервер і централізовано обробляються. Такі програми, як запити бази даних, можуть скористатися перевагою обчислювальної потужності хоста, не залежачи від відносно обмеженої потужності віддаленої системи.
- Віддалене управління підтримує корпоративні інвестиції в старі і повільніші робочі станції, портативні ПК і модеми. Оскільки віддалене управління не вимагає локальної обробки, не обов'язково оснащувати кожного віддаленого користувача потужними комп'ютерами, високопродуктивними дисководами та швидкими модемами.

• Немає необхідності в додатковому ліцензуванні програмного забезпечення, оскільки віддалена система не вимагає додаткового програмного забезпечення. Вся обробка відбувається на хост-системі.

У той же час віддалений доступ має певні недоліки:

• Продуктивність, як правило, погана при використанні графічних додатків, таких як Microsoft Windows, електронних таблиць або програм для обробки зображень, через те, що зображення та екрани передаються по комутованих лініях.

• Віддалені користувачі не можуть отримати доступ до мережевих послуг, як якщо б вони були безпосередньо підключені до локальної мережі, і часто потрібно вивчати нові методи доступу до мережевих послуг через систему хоста.

• Реалізація віддаленого управління створює технічні проблеми. Хост-система повинна працювати, щоб віддалений користувач міг скористатися перевагами програмного забезпечення, яке знаходиться в ньому. Якщо хост-система вимкнена або виникає проблема, віддалений користувач не в змозі працювати.

• З усіма методами віддаленого управління безпека викликає занепокоєння. При використанні віддаленого управління на моніторі хост-системи відображається вся інформація, яка обробляється дистанційно, що дозволяє випадковому спостерігачеві переглядати всю діяльність на екрані, включаючи електронну пошту та конфіденційну інформацію.

• Віддалений користувач може отримувати доступ і запускати електронну пошту або інші програми тільки під час підключення до хост-системи через лінію набору. Вся робота повинна виконуватися по комутованій лінії.

Навіть з цими обмеженнями, для віддаленого введення даних і невеликих передач файлів, метод віддаленого управлінням може бути ефективним і економічним рішенням.

Аналіз методу віддаленого вузла

Донедавна віддалене управління було методом віддаленого доступу. Однак, з впровадженням потужних портативних ноутбуків, доступних швидких модемів, мостів і маршрутизаторів, більш просунутих алгоритмів стиснення і клієнт-серверних додатків, віддалений вузол набирає популярність. За допомогою віддаленого вузла безліч ПК на різних локаціях посилаються на сервер головного офісу, що дозволяє їм працювати як би безпосередньо приєднане до корпоративної локальної мережі [4]. Принцип роботи віддаленого вузла проілюстрований на Рис.1.4

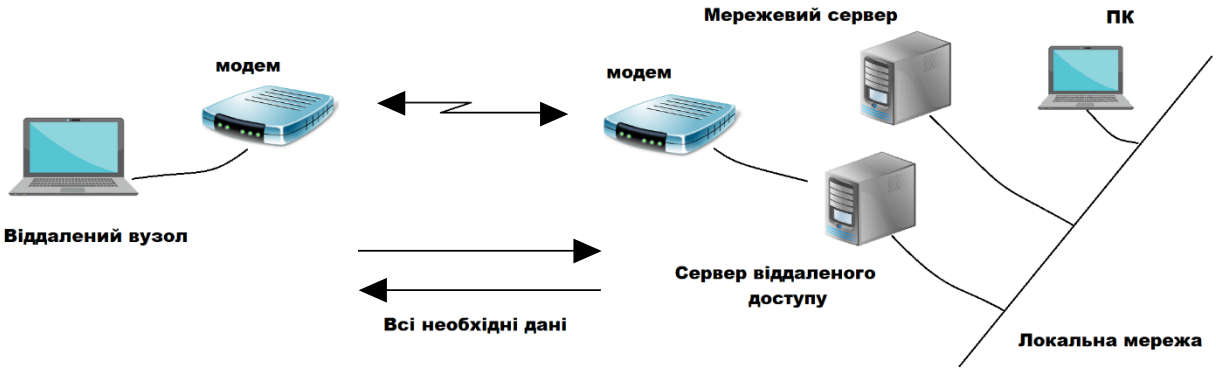


Рис.1.4 Принцип роботи віддаленого вузла

Промислові тенденції до клієнт-серверних додатків та графічних додатків, заснованих на графічному інтерфейсі, зумовлюють попит на рішення віддалених вузлів. Архітектура віддаленого вузла схожа на архітектуру клієнт-сервер. Віддалена система діє як клієнт та сервер зв'язку, який надає доступ до

потрібного сервера. Програми або частини програм обробляються на віддаленій системі. Через лінію передаються лише дані мережі, такі як електронна пошта. Оскільки вузол віддаленого доступу є прозорим, він є методом доступу до клієнта / сервера.

Віддалений вузол дозволяє користувачам підключатись до мережі та отримувати доступ до локальної мережі, так якщо б вони були локально приєднані. Хоча доступ є більш повільним, користувач може отримати доступ до файлового сервера безпосередньо, замість того, щоб переносити файл на локальний диск, який необхідний для метода віддаленого керування. Для редагування документа на мережевому диску, наприклад, віддалений користувач просто відкриває його замість того, щоб передати документ на локальний диск. Це робить віддалений вузол набагато простішим у використанні, ніж дистанційне керування.

Бажано, щоб на віддаленому ПК крім мережевого системного програмного обладнання знаходилося все прикладне програмне забезпечення, необхідне для сеансу зв'язку: всі виконувані файли, необхідні програми. В іншому випадку їх необхідно буде передавати з мережевого сервера на канал зв'язку. Вони мають, як правило, великі обсяги даних, отже це потребуватиме значних витрат часу.

Як кожен повноцінний користувач локальної мережі, віддалений вузол має свою мережеву адресу. Мережева операційна система перетворює мережеві пакети, які потрібно передати через модем, з формату протоколу IP або IPX в формат, сумісний зі стандартом послідовної передачі. З появою все більшої кількості програм, що підтримують архітектуру "клієнт - сервер", посилюється тенденція на програмне забезпечення для віддалених вузлів. Такі програми

дозволяють обробляти великі файли даних на серверах локальної мережі, а на віддалений ПК передавати тільки результат обробки.

Віддалена система виконує клієнтські функції, а сервери домашнього офісу виконують справжні функції сервера. Це дозволяє віддаленим користувачам скористатися перевагою віддаленої обробки для реалізації графічних додатків. У той час як віддалений доступ передбачає підключення безпосередньо до хост-системи, віддалений вузол підключається до віддаленого сервера доступу. При підключенні до корпоративної мережі, мережеві ресурси виглядають локальними, як якщо б віддалений користувач був безпосередньо підключений до локальної мережі.

Віддалений вузол має наступні переваги:

- Продуктивність краще з цим методом, ніж з методом віддаленого керування при використанні графіки та додатків, оскільки зображення на екрані не передаються через лінію.

- Віддаленим користувачам не потрібно перенавчатися, щоб отримати доступ до мережевих ресурсів або використовувати віддалені програми. Користувач пов'язаний з комп'ютером і мережею, як якщо б вони були безпосередньо підключені до локальної мережі.

- Продуктивність віддалених користувачів не залежить від підключення до корпоративного відділення. Програми резидентні на віддаленій системі і можуть працювати незалежно.

- Оскільки продуктивність користувачів не повністю залежить від віддаленого підключення, тарифи на основі ліній зв'язку можна звести до мінімуму. Наприклад, при віддаленому доступі до електронної пошти віддалений користувач не зобов'язаний підтримувати відкрите підключення до телефонної лінії до корпоративного відділення під час перегляду повідомлень.

Користувач може встановити з'єднання для завантаження повідомлень, відключити лінію, а потім прочитати повідомлення в автономному режимі на попередньому екрані зручніше. Це дає можливість скоротити час підключення, що призводить до зниження витрат.

Віддалений вузол також має свої недоліки:

- Віддалений вузол вимагає додаткового ліцензування прикладного програмного забезпечення для кожного віддаленого користувача, оскільки програми виконуються незалежно від кожної віддаленої системи.
- Віддалений вузол вимагає інвестицій у більш потужні віддалені комп'ютери, більш високі накопичувальні диски і більш швидкі модеми, мости або маршрутизатори.

Оскільки користувачі віддаленого вузла отримують доступ до мережі, як якщо б вони були локально приєднані, небажані вторгнення здатні переміщатися по мережі без вивчення складних процедур доступу.

1.2 Дослідження проблем безпеки при віддаленому доступі

Невід'ємною властивістю систем віддаленого доступу є наявність глобальних з'єднань. За своєю суттю глобальні комунікації, які простягаються на десятки і тисячі кілометрів, не заважають зашкодити доступу до даних, що передаються по цих лініях. Не може бути ніякої гарантії, що в деяких, недоступних для керування точка простору, дехто, наприклад, користуючись аналізатором протоколів, не підключиться до носія передачі, щоб перехватити та декодувати пакетні дані. Це однаково небезпечно для всіх типів територіальних каналів і не пов'язано з використанням власних, орендованих каналів зв'язку або послуг громадських наземних мереж, таких як Інтернет. Але використання глобальних мереж ще більше погіршує ситуацію, в цьому випадку для зловмисника доступ до даних є більш різноманітнішим та

зручнішим. Тому отримати доступ до даних може більша кількість користувачів.

Безпечна система -

це система, що надійно зберігає інформацію та завжди може надавати її користувачам , та система, яка захищає дані від зловмисників.

Брандмауер (firewall) - пристрій, що представляє собою універсальний комп'ютер, який має спеціальне ПЗ, встановлене на ньому, який розташований між захищеною (внутрішньою) мережею та глобальними мережами. Брандмауер контролює всі потоки інформації між внутрішніми та глобальними мережами, пересилаючи дані відповідно до попередньо визначених правил. Ці правила є формальним виразом політики безпеки, затвердженими в компанії. Брандмауери засновані на двох основних методах безпеки: фільтрація пакетів, посередницькі послуги (proxy-services). Ці дві функції можна використовувати як окремо, так і в комбінації.

Пакетна фільтрація. Використання маршрутизаторів як брандмауера

Фільтрація здійснюється на транспортному рівні: всі ті, хто проходить через пакети брандмауера, аналізуються, інші, що мають певні ("неавторизовані") значення в деяких полях, відкидаються.

Пропуск у внутрішню мережу пакетів мережевого рівня чи кадрів канального рівня за адресами (MAC-адреси, IP-адреси, IPX-адреси) або номерами портів TCP, даних додатків. Наприклад, щоб трафік telnet не заходив за межі внутрішньої мережі, брендмауер повинен фільтрувати всі пакети, в заголовку TCP яких вказана адреса порту процесу-одержувача, рівний 23 (цей номер зарезервований за сервісом telnet). Важче відстежувати трафік FTP, що працює з великим діапазоном можливих номерів портів, що вимагає завдання більш складних правил фільтрації.

Для фільтрації пакетів також використовується простий маршрутизатор, справді, на базі маршрутизаторів працюють багато пакетних фільтрів. Брандмауери забезпечують більш надійний захист даних ніж маршрутизатори. Фільтрація фаєрволом є краща за фільтрацію маршрутизатором. Головні переваги це: брандмауер має кращі логічні здібності, брандмауер має велику кількість можливостей аудиту всіх подій, які пов'язані з безпекою.

Проксі - сервіси (Proxy-services). Проксі послуги не дозволяють пряму передачу трафіку між внутрішніми та зовнішніми мережами. Щоб зв'язатися з віддаленою службою, клієнт-користувач локальної мережі визначає логічне з'єднання з проксі службою, що працює на брандмауері. Послуга проксі встановлює окреме підключення до "істинної" служби, працюючи на сервері зовнішньої мережі, отримує відповідь від неї і відправляє її клієнту, користувачеві локальної мережі, до призначеного пункту призначення.

Для кожної послуги потрібна спеціальна програма: проксі-сервіс. Зазвичай екран безпеки включає в себе проксі послуги для FTP, HTTP, TELNET. Багато захисних екранів мають засоби для створення проксі програм для інших служб. Деякі реалізації проксі послуг вимагають, що клієнт мав спеціальне ПЗ. Наприклад: Sock - Широко використовуваний набір інструментів для створення проксі програм.

Проксі-сервіси не тільки відправляють сервісні запити, наприклад, розроблений посередником CERN (із фр. Organisation européenne pour la recherche nucléaire), що працює під протоколом HTTP, може накопичувати дані в кеш брандмауера, так що користувачі внутрішньої мережі можуть отримувати дані з набагато швидше.

Журнали подій, які підтримуються проксі службами, можуть допомогти запобігти вторгненню на основі записів регулярних невдалих спроб. Іншою

важливою особливістю проксі послуг, що позитивно впливає на безпеку системи, є те, що коли брандмауер відмовляється захищатися проксі послугою, оригінал залишається недоступним.

Проксі - сервіси надійніші фільтрів, але вони мають меншу продуктивність обміну даними між внутрішньою і зовнішньою мережами, вони також не володіють тим ступенем прозорості для додатків та кінцевих користувачів, що властиво для фільтрів.

Використовуючи технологію захищеного каналу дані, що передаються по доступній транспортній мережі (наприклад, інтернет) мають бути забезпечені заданим рівнем безпеки. Для цього повинні виконуватись три основні функції: взаємна аутентифікація абонентів, захист від несанкціонованого доступу повідомлення, що передаються по каналу, підтвердження цілісності, що надходить по каналу повідомлення.

Взаємна аутентифікація двох сторін під час встановлення з'єднання може виконуватися, наприклад, обміном сертифікатами. Для забезпечення секретності можна використовувати будь-який метод шифрування. Наприклад, симетричні сеансові ключі використовують для шифрування переданих повідомлень. Сеансові ключі шифруються використовуючи відкриті ключі. Симетричні ключі мають більшу швидкість шифрування та дешифрування процесів, ніж асиметричні. Для того, щоб досягти цілісність повідомлень потрібно до повідомлення, яке не зашифроване сесійним ключем додати дейджест.

Безпечний канал у загальнодоступній мережі часто називають віртуальною приватною мережею (VPN). Існує два способи утворення VPN (Рис.2.1): за допомогою спеціального ПЗ кінцевих вузлів, за допомогою

спеціального ПЗ для шлюзів, що знаходяться на межі між приватними та громадськими мережами.

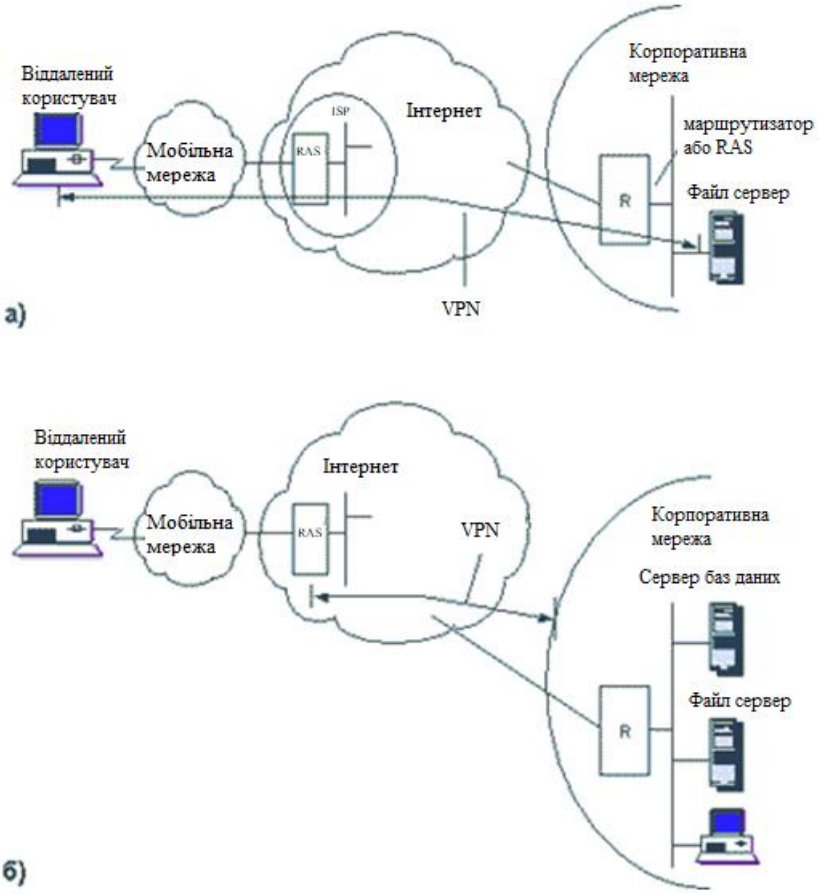


Рис. 2.1, а) Утворення VPN за допомогою спеціального ПЗ кінцевих вузлів, б) Утворення VPN за допомогою спеціального ПЗ для шлюзів.

У випадку, що на (Рис.2.1, а) програмне забезпечення, встановлене на віддаленому клієнтському комп'ютері, встановлює безпечний канал з корпоративним мережевим сервером, до якого клієнт звертається до ресурсів. У цьому способі перевагою є повний захист каналу по всьому маршруту та можливість використовувати різні протоколи для створення безпечних каналів. Недоліками є надмірність і децентралізація рішення. Надмірність проявляється

в тому, що найбільш уразливими в основному є мережі з комутацією пакетів, а не канали безпровідної мережі чи виділені канали. Встановлення програмного забезпечення на всі клієнтські комп'ютери та сервери локальної мережі не є обов'язковим. Децентралізація не дає можливості централізовано управляти ресурсами мережі. Адмініструвати кожний сервер та кожний комп'ютер користувача для конфігурації в них засобів захисту даних у великій мережі важко та не зручно.

У іншому випадку (Рис.3.1, б) клієнти та сервери не створюють захищений канал - це закладено тільки всередині загальнодоступної мережі з комутацією пакетів. Канал створюється між постачальником послуг віддаленої загальнодоступної мережі і маршрутизаторам корпоративної мережі. Реалізація такого підходу складніша - вона вимагає стандартного протоколу для створення захищеного каналу, встановлення програмного забезпечення, що підтримує такий протокол, всім провайдерам необхідно підтримувати протокол виробниками віддалених серверів і маршрутизаторів доступу.

1.3 Аналіз технології VPN

Віртуальна приватна мережа (VPN) становить собою підключення типу «точка-точка» в приватній або глобальній мережі. VPN-клієнти використовують спеціальні TCP / IP-протоколи, звані тунельними протоколами, що забезпечують встановлення захищеного каналу обміну даними між двома комп'ютерами. З точки зору комп'ютерів, що взаємодіють між ними організовується виділений канал типу «точка-точка», хоча насправді, відповідні дані передаються через інтернет, як і будь-які інші пакети. При підключенні до віддаленого сервера VPN клієнт створює віртуальний канал «точка-точка» через інтернет [6]. Сервер віддаленого доступу приймає виклик, робить перевірку

аутентифікації сторони, що викликає та пересилає дані між локальною мережею компанії та VPN-клієнтом. Приклад VPN-підключення показаний на Рис.1.5.

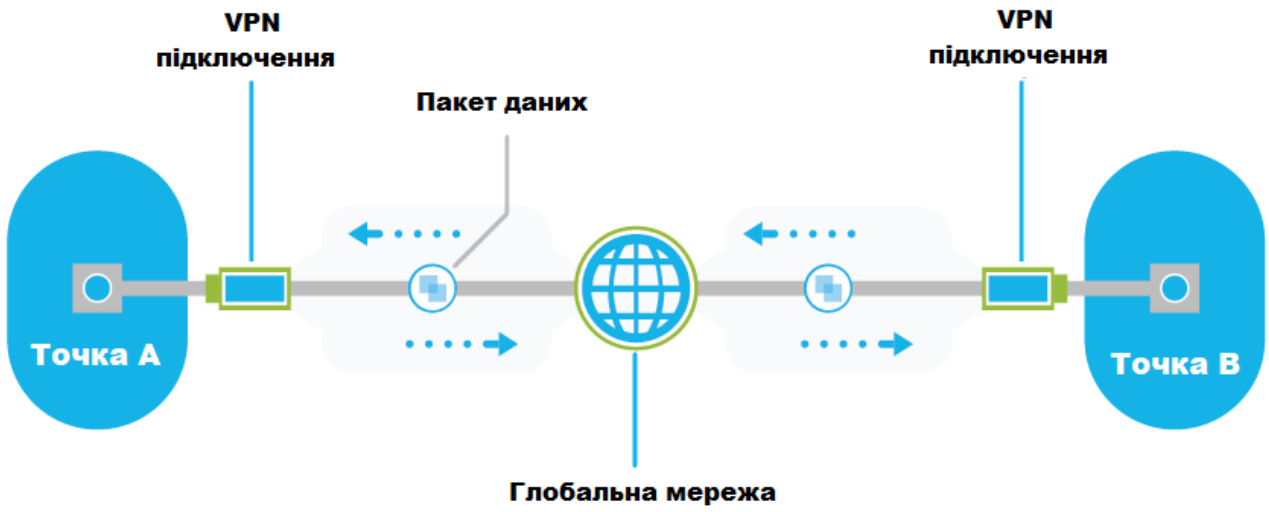


Рис.1.5 VPN-підключення

Існує два типи VPN-підключень:

VPN-підключення віддаленого доступу. VPN-підключення віддаленого доступу дає користувачам можливість працювати вдома або в дорозі, отримуючи доступ до сервера приватної мережі за допомогою інфраструктури глобальної мережі. Для підключення VPN користувача існує зв'язок "точка-точка" між клієнтським комп'ютером і сервером організації. Реальна інфраструктура загальної або публічної мережі не має значення, так як дані передаються подібно до того, як якщо б вони передавалися по виділеному приватному каналу.

VPN-підключення типу «мережа-мережа». VPN-підключення типу «мережа-мережа» (іноді називається VPN-підключенням типу «маршрутизатор-маршрутизатор») призначено для маршрутизації підключень між різними філіями організації, а також між організаціями через загальнодоступну мережу,

забезпечуючи при цьому захист підключень. Якщо мережі з'єднані через Інтернет, як показано на наступному малюнку, маршрутизатор з підтримкою VPN пересилає пакети іншому такому маршрутизатору через VPN-підключення. З точки зору маршрутизаторів VPN-підключення на логічному рівні функціонує як виділений канал рівня передачі даних.

За допомогою VPN-підключень можливо з'єднати дві приватні мережі. VPN-сервер забезпечує маршрутизацію підключення до мережі, до якої приєднано VPN-сервер. Маршрутизатор який робить виклик проходить перевірку аутентифації на відповідальному маршрутизаторі, та в цілях взаємної перевірки аутентифікації маршрутизатор, який відповідає робить перевірку аутентифікації на маршрутизаторі який робив виклик. При VPN - підключення типу «мережа-мережа» пакети, що відправляються з будь-якого з маршрутизаторів через VPN-підключення, зазвичай формуються не на маршрутизаторах. На Рис.1.6 представлено VPN-підключення між двома віддаленими сайтами через Інтернет.

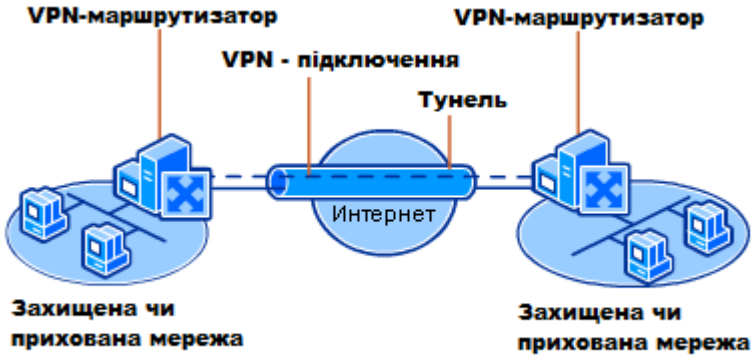


Рис.1.6 VPN-підключення між двома віддаленими сайтами через Інтернет

Властивості VPN-підключення:

Інкапсуляція. Забезпечується інкапсуляція приватних даних з використанням заголовка, який має в собі відомості про маршрутизації для передачі цих даних по транзитній мережі.

Перевірка аутентифікації. Існує три різні форми перевірки аутентифікації для VPN-підключень.

Перевірка аутентифікації на рівні користувача по протоколу PPP (Point-to-Point Protocol). Для встановлення VPN-підключення VPN-сервер виконує перевірку аутентифікації VPN-клієнта, що намагається встановити підключення, на рівні користувача по протоколу PPP і перевіряє, чи має VPN-клієнт відповідні дозволи на доступ. При взаємній перевірці аутентифікації VPN-клієнт також виконує перевірку справжності VPN-сервера, що гарантує захист від комп'ютерів, що видають себе за VPN-сервери [7].

Перевірка автентичності на рівні комп'ютера по протоколу IKE (Internet Key Exchange). Щоб встановити співставлення безпеки IPSec, VPN-клієнт і VPN-сервер використовують протокол IKE для обміну сертифікатами комп'ютерів або попередньо ключем. В обох випадках VPN-клієнт і VPN-сервер виконують взаємну перевірку аутентифікації на рівні комп'ютера. Перевірка аутентифікації на основі сертифікату комп'ютера є одним з найнадійніших способів і рекомендується до застосування. При перевірці аутентифікації на рівні комп'ютера використовуються підключення по протоколам L2TP / IPSec або IKE версії 2.

Перевірка аутентифікації джерела даних і забезпечення цілісності даних. Щоб переконатися в тому, що джерелом відправлених по VPN-підключенню даних є інша сторона VPN-підключення і що вони передані в незміненому вигляді, в дані включається контрольна сума шифрування, заснована на ключі

шифрування, який відомий тільки відправнику та одержувачу. Функції перевірки проходження даних і забезпечення цілісності даних доступні для підключень по протоколах L2TP / IPSec і IKE версії 2.

Шифрування даних. Для забезпечення конфіденційності даних при передачі по загальній або публічній транзитивній мережі вони шифруються відправником і розшифровуються одержувачем. Успішність процесів шифрування і розшифрування гарантується в тому випадку, коли відправник і одержувач використовують загальний ключ шифрування.

Висновки

1. Розглянуті методи віддаленого доступу. Був проведений аналіз методів: термінального доступу, віддаленого управління та віддаленого вузла. Були виявлені головні переваги та недоліки даних методів.

2. Виявлені проблеми захисту інформації при організації віддаленого доступу. Був описаний принцип роботи брандмауера та його методи безпеки: фільтрація пакетів та проксі - послуги.

3. Проаналізовано технологію VPN. Було досліджено два типи VPN-підключень: підключення віддаленого доступу, підключення типу «мережа-мережа». Розглянуті властивості VPN-підключення.

РОЗДІЛ 2
ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Огляд можливих заходів для забезпечення безпеки при віддаленому доступі

Безпека є серйозною проблемою в більшості мережевих середовищ, але особливо коли віддалений доступ надається мобільним користувачам та філіям. Користуючись віддаленим доступом можливо натрапити на хакерів, які схильні до підробки або крадіжки конфіденційної інформації [5]. Повинні бути вжиті відповідні запобіжні заходи, щоб не допустити серйозних втрат користуючись віддаленим доступом.

Залежно від розміру мережі та важливості інформації, до якої можливо отримати віддалений доступ, можна використовувати один або кілька методів безпеки.

Аутентифікація. Це передбачає перевірку віддаленого абонента за допомогою ідентифікатора користувача та пароля, таким чином контролюючи доступ до сервера. Безпека посилюється, якщо ID і паролі шифруються перед виходом по каналу зв'язку.

Обмеження доступу. Це передбачає призначення кожному віддаленому користувачеві певного розташування (тобто каталогу або диска), до якого можна звертатися на сервері. Доступ до конкретних серверів можна навіть контролювати.

Обмеження часу. Для кожного віддаленого користувача дається певний час для сеансу. Після завершення часу сеанс переривається.

Обмеження підключення. Кількість спроб підключення є обмежений. Наприклад коли можливо ввести певну кількість спроб за тиждень чи за день.

Обмеження протоколу. Це передбачає обмеження користувачів певним протоколом для віддаленого доступу.

Зворотній зв'язок. При зворотному виклику приймається дзвінок клієнта, лінія відключається, та сервер передзвонює для клієнта після перевірки правильності номера телефону. Цей метод є хороший для філій, але в інших випадках він не завжди є хорошим рішенням. Для тих хто змінює своє місцезнаходження постійно.

Шифрування. Коли бездротові послуги використовуються для віддаленого доступу, шифрування є важливим для захисту конфіденційної інформації, оскільки вона перетинає ефір. Пристрої на обох кінцях запускають програмне забезпечення для кодування і декодування інформації. Незважаючи на те, що програмне забезпечення для шифрування є додатковою витратою при користуванні послугами пакетного радіозв'язку, нова бездротова послуга, заснована на технології стільникового цифрового пакетного передавання даних, використовує аутентифікацію та шифрування як цілісні функції, що перешкоджає випадковому перехопленню [4].

2.2 Використання технології vpn для забезпечення інформаційної безпеки

VPN не була першою технологією для віддаленого підключення. Раніш найбільш поширений спосіб підключення комп'ютерів між декількома офісами полягав у використанні виділеної лінії. Орендовані лінії, такі як ISDN (Digital Network Integrated Services, 128 Кбіт / с), - це приватні мережеві з'єднання, які телекомунікаційна компанія може орендувати своїм клієнтам. Орендовані лінії надали компанії можливість розширити свою приватну мережу за межами її безпосереднього географічного району. Ці з'єднання утворюють єдину глобальну мережу (WAN) для бізнесу. Незважаючи на те, що орендовані лінії

надійні, оренда коштує дорого, із збільшенням відстані між офісами витрати зростають.

Сьогодні Інтернет є більш доступним, ніж будь-коли раніше, і Інтернет-провайдери продовжують розвивати швидші, надійніші послуги за нижчою вартістю, ніж орендовані лінії. Щоб скористатися цим, більшість підприємств замінили орендовані лінії новими технологіями, що використовують підключення до Інтернету, не жертвуючи продуктивністю та безпекою. Підприємства почали з створення інтрамереж, які є приватними інтрамережами, призначеними для використання лише працівниками компанії. Інтернет дозволив віддаленим колегам працювати разом, використовуючи такі технології, як спільний доступ до робочого столу. Додаючи VPN, підприємства можуть розширити свої ресурси інтрамережі, дозволяючи працівникам працювати з віддалених офісів або будинків.

Мета VPN - забезпечити безпечне та надійне з'єднання між комп'ютерними мережами через існуючу загальнодоступну мережу, як правило, Інтернет.

Добре розроблена VPN забезпечує наступні переваги:

- Розширені зв’язки в різних географічних місцях без використання виділеної лінії.
- Підвищена безпека обміну даними.
- Гнучкість для віддалених офісів та співробітників щодо використання інтрамережі через існуюче підключення до Інтернету, як якщо б вони були безпосередньо підключені до мережі.
- Економія часу та грошей.
- Підвищена продуктивність для географічно розподілених ресурсів.

У той же час від VPN завжди потрібно:

- Безпека. VPN повинен захищати дані під час подорожі у загальнодоступній мережі. Якщо зловмисники намагаються викрасти дані, вони не зможуть їх прочитати або використовувати.
- Надійність. Співробітники та віддалені офіси повинні мати можливість підключатися до VPN без будь-яких проблем, і VPN повинна забезпечувати однакову якість з'єднання для кожного користувача, навіть коли він обробляє максимальну кількість одночасних з'єднань.
- Масштабованість. Послуги VPN повинні бути розширюваними.

Віртуальна приватна мережа - це захищений тунель між двома або більше комп'ютерами в Інтернеті, що дозволяє їм отримувати доступ один до одного, як і в локальній мережі. Раніше VPN використовувались в основному компаніями для надійного підключення віддалених відділень або підключення роумінгових працівників до офісної мережі, але сьогодні вони також є важливою послугою для споживачів, захищаючи їх від атак при підключенні до загальнодоступних бездротових мереж.

Відкриті бездротові мережі становлять серйозну загрозу для користувачів, оскільки зловмисники в одних і тих же мережах можуть використовувати різні методи для моніторингу веб-трафіку і навіть викрадати облікові записи на сайтах, які не використовують протокол безпеки HTTPS. Крім того, деякі оператори мережі Wi-Fi навмисно вводять рекламу у веб-трафік, що може призвести до небажаного відстеження.

У деяких регіонах світу уряди контролюють користувачів, які відвідують певні веб-сайти, з метою виявлення політичної приналежності та дисидентів - практики, яка загрожує свободі слова та правам людини.

Використовуючи VPN-з’єднання, весь трафік можна безпечно маршрутизувати через сервер, розташований в інших місцях світу. Це захищає

від локальних спроб відстеження та злому та навіть приховує справжню адресу Інтернет-протоколу від веб-сайтів та служб, до яких здійснюється доступ.

Існують різні технології VPN з різним ступенем шифрування. Наприклад, протокол туннелювання точка-точка (PPTP) є швидким, але набагато менш безпечним, ніж інші протоколи, такі як IPSec або OpenVPN, який використовує SSL / TLS (Secure Sockets Layer / Transport Layer Security). Крім того, при використанні VPN на основі TLS важливий також тип алгоритму шифрування та довжина ключа.

Хоча OpenVPN підтримує безліч комбінацій шифрів, протоколів обміну ключами та алгоритмів хешування, найпоширенішою реалізацією, яку пропонують провайдери VPN для з’єднань OpenVPN, є шифрування AES із обміном ключами RSA та підписами SHA. Рекомендованими варіантами є шифрування AES-256 із ключем RSA щонайменше 2048 біт та криптографічною хеш-функцією SHA-2 (SHA-256) замість SHA-1.

Варто зазначити, що шифрування може вплинути на швидкість з'єднання. Вибір технології VPN та методів шифрування слід робити в кожному конкретному випадку, залежно від того, які дані будуть передані.

VPN також використовується для доступу до вмісту в Інтернеті, який недоступний у певних регіонах, хоча це залежить від того, наскільки власники вмісту дотримуються обмежень. Постачальники послуг VPN зазвичай використовують сервери в багатьох країнах світу і дозволяють користувачам легко переключатися між ними. Наприклад, користувачі можуть підключатися через сервер в одній країні, щоб отримати доступ до обмеженого вмісту у своїй або іншій країні.

Користувачі таких країн, як Китай або Туреччина, де уряди регулярно блокують доступ до певних веб-сайтів з політичних причин, зазвичай використовують VPN для обходу цих обмежень.

Розгортаючи VPN на міжнародному рівні, вам потрібно переконатися, що закони та правила різних країн не порушуються, оскільки послуги VPN там можуть бути обмежені.

Правила можуть орієнтуватися на споживачів, які намагаються відвідувати заборонені веб-сайти, але вони також можуть застосовуватися до підприємств, які підключаються до філій в інших місцях. Суть полягає в тому, щоб перевірити закони в усіх країнах, де розміщується сайт VPN, щоб переконатися, що він є законним та чи існують правила, які можуть порушити конфіденційність [8].

У міру зростання різноманітності та інтенсивності кіберзагроз адміністраторам мереж потрібно збалансувати бажання повністю заблокувати внутрішні мережі своєї організації від доступу до Інтернету, одночасно забезпечуючи повсюдний доступ до внутрішньої мережі з багатьох віддалених пристроїв, співробітників, клієнтів та IoT. Цього балансу можна досягти за допомогою використання віртуальної приватної мережі (VPN), яка використовує Інтернет для забезпечення безпечного доступу до віртуальної мережі.

Кращим способом очищення конфіденційних даних та додатків є надання доступу до них за допомогою “нестандартної доступності”, наприклад, Інтернету. Мережі, які враховують інфраструктуру, в якій дані конфіденційності зберігаються, ізольовані від Інтернету, з метою їх захисту відображаються IP-адреси, недоступні через Інтернет. Безпека посилюється за рахунок обмеження доступу до ряду посилань, тому доступ до них може оброблятись лише від

співочого трафіку лише з дозволених зовнішніх вкладень. Як поодинокі, так і переплетені огорожі називаються «приватними огорожами».

Підприємство може мати приватну мережу, яка пов'язує всю свою IT-інфраструктуру та комп'ютери службовців з корпоративною інтрамережею. Ця мережа дозволяє отримати доступ до всіх внутрішніх IT-послуг, таких як заробітна плата, електронна пошта тощо, у штаб-квартирі підприємства. У міру зростання бізнесу приватну мережу можна також розширити до додаткових філій.

Спеціальний транспорт даних за орендованими лініями зв'язку часто використовується для встановлення зв'язку між офісами для їх приватної мережі, зберігаючи мережу окремо від Інтернету. Телекомунікаційні послуги, що використовуються для створення цього зв'язку між місцезнаходженнями, є досить дорогими, і потрібні більш економічні альтернативи.

Для встановлення зв'язку між офісами, для їх приватної мережі при збереженні мережі окремо від інтернету часто використовується виділений транспорт даних з орендованими лініями електрозв'язку. Телекомунікаційні послуги, які використовуються для створення зв'язку з цим між місцями розташування, досить дороги і необхідні більш економічні альтернативи.

Завдяки досягненням в області криптографії, обчислювальної техніки та інтернету стало можливим шифрувати трафік даних і тунелювати його через інтернет на сервер, розташований в приватній мережі. Захищений тунель створює віртуальну зв'язок, який розширює приватну мережу через загальнодоступну мережу.

VPN може використовувати одну з багатьох технологій, таких як Інтернет-протокол (IPsec), безпека транспортного рівня (SSL /TLS), безпека транспортного рівня даних (DTLS), надійно підключаючи пристрої або мережі

через загальнодоступні мережі для розширення або формування приватної мережі.

Ті самі технології, які використовуються для створення віртуального зв’язку між мережами, також можуть бути використані для підключення пристроїв користувача до приватної мережі. Загальне використання VPN полягає в забезпеченні віддалених працівників безпечним доступом до Інтернету до IT-послуг своєї компанії. Співробітники використовують VPN-клієнтів, встановлених на корпоративних ноутбуках або мобільних пристроях, для підключення до VPN-сервера, який присутній в приватній мережі компанії.

Випадок використання віддаленого доступу не обмежується доступом співробітників. Будь-який пристрій, підключений до Інтернету, може використовувати VPN, щоб бути частиною приватної мережі. Пристрої можуть варіюватися від звичайних обчислювальних пристроїв, таких як ноутбуки, до спеціалізованих промислових датчиків або побутової електроніки, таких як смарт-телевізори.

Чим більше пристроїв і послуг підключення до глобальної мережі, загроза кібератак збільшується. Доступ VPN до потрібних вам пристроїв допомагає зменшити потенційні загрози. Правильно реалізована VPN дозволяє лише довіреним пристроям отримати доступ до приватної мережі та застосовує надійні засоби контролю доступу для забезпечення найменш привілейованого доступу. Ці заходи зменшують кількість атак, доступних для хакерів, щоб порушити безпеку мережі.

Рішення VPN також забезпечують взаємну автентифікацію, при якій як VPN-сервер, так пристрій, що підключає автентифікують один одного. У разі успіху користувач, що підключається до мережі, автентифікує з використанням імені користувача / пароля і, необов'язково, з використанням іншої форми

автентифікації, яка може бути токеном безпеки, наприклад за допомогою мобільного телефону або смарт-карти. Після того, як пристрій і користувач ідентифікуються, сервер VPN може визначати правила доступу, так що користувач отримує тільки доступ до підмножини систем / послуг, до яких вони мають право доступу.

Ще однією перевагою безпеки використання VPN є шифрування даних, яке захищає від прослуховування та втрати даних.

Сьогодні використання послуг SaaS набирає популярність. Що також може забезпечити розподілене використання ресурсів.

Але не всі програми SaaS пропонують досить високий рівень безпеки. Зазвичай додатки SaaS покладаються тільки на автентифікацію імені користувача та пароля. Якщо ви не будете слідувати рекомендації щодо забезпечення безпеки для захисту пароля та блокування облікового запису при невдалих спробах, для отримання несанкціонованого доступу можна використовувати грубі атаки та експлуатування на слабких механізмах відновлення пароля. Тому доцільно дозволити примусові політики корпоративної безпеки за допомогою VPN для підключення до корпоративної мережі, а потім доступу до додатків SaaS через корпоративну мережу.

HTTPS також не можна розглядати як альтернативу VPN. HTTPS не можна використовувати безперервно протягом усього сеансу веб-перегляду. Зазвичай він використовується лише на певних сайтах і лише для певних транзакцій, які передають конфіденційну інформацію, таку як ім’я користувача / пароль або дані кредитної картки. HTTPS добре захищає конфіденційну інформацію під час використання, але VPN найкраще тримає весь сеанс перегляду конфіденційним та захищає весь трафік при підключенні до ненадійних мереж. HTTPS використовує TCP та забезпечує захист веб-додатків.

Таким чином, він не може забезпечити трафік з усіх не інтернет-програм, які можна використовувати на пристрої, таких як електронна пошта або VoIP, та потокових програм, які не покладаються на TCP, таких як Skype або Spotify. За допомогою VPN можна захистити весь трафік із пристрою, незалежно від програми, що генерує трафік. Будучи захищеним транспортним протоколом для конкретних додатків, HTTPS не діє як VPN і, отже, не може забезпечити всіх переваг VPN, таких як доступ до спільних файлів, мережевих принтерів та інших мережевих ресурсів у більшій приватній мережі.

Основна мета VPN - забезпечити безпечний доступ до приватної мережі без безпосереднього підключення до фізичної приватної мережі. Таким чином, VPN розширює всі послуги, доступні в приватній мережі, як якщо б пристрої були безпосередньо підключені до приватної мережі.

Корпоративні IT-спеціалісти можуть надавати такі послуги, як файлові сервери, сервери друку, веб-сайти інтрамережі, ERP-системи, резервні сервери тощо. Ці послуги призначені лише для внутрішнього використання, але з VPN працівник не обмежується фізичним місцезнаходженням і може мати пряме підключення до внутрішньої IT-мережі з будь-якого географічного розташування.

Ця ж приватна мережа може надавати спеціалізовані послуги для підключених до Інтернету пристроїв, таких як IP-телефонія або управління пристроями. VPN можна використовувати для надійного підключення цих пристроїв до обчислювальної інфраструктури, яка надає спеціалізовані послуги через приватну мережу. VPN - відмінне рішення для безпечної передачі даних, що передаються та приймаються різними пристроями.

Ви також повинні розуміти, що з VPN також існують ризики безпеки. Сюди входять викрадення VPN, при якому неавторизований користувач

викрадає з’єднання VPN з віддаленого клієнта, атаки «посередині», в яких зловмисник може перехоплювати дані, слабка автентифікація користувача, роздільне тунелювання, в якому користувач отримує доступ до небезпечного з’єднання з Інтернетом, а також доступ до підключення до приватної мережі VPN, зараження шкідливим програмним забезпеченням на клієнтському комп’ютері, надання занадто великих прав доступу до мережі та витоки DNS, коли комп’ютер використовує DNS-з'єднання за замовчуванням, а не захищений VPN-сервер DNS[9].

Щоб усунути ці ризики, вам слід розглянути додаткові функції безпеки VPN, вибираючи продукт VPN. Сюди входять обов’язкові засоби безпеки:

- Підтримує надійну автентифікацію.
- Надійні алгоритми шифрування.
- Використання антивірусного програмного забезпечення та засобів виявлення та запобігання вторгненню.
- Надійний захист за замовчуванням для портів адміністрування та обслуговування.
- Підтримка цифрового сертифіката.
- Підтримка реєстрації та аудиту.
- Можливість призначати адреси клієнтам у приватній мережі, зберігаючи всі адреси приватними.

Крім того, адміністратори мережі та безпеки, персонал довідкової служби та віддалені користувачі повинні бути навчені дотримуватися найкращих практик безпеки під час розгортання та постійного використання VPN.

Інший спосіб поліпшити безпеку VPN - це Perfect Forward Secrecy (PFS). Якщо використовується PFS, зашифровані повідомлення та сеанси, записані в

минулому, не можуть бути отримані та розшифровані, якщо довгострокові секретні ключі або паролі порушені.

За допомогою PFS кожен сеанс VPN використовує різну комбінацію ключів шифрування, тому навіть якщо зловмисники викрадуть один ключ, вони не зможуть розшифрувати будь-які інші сеанси VPN.

Існує чотири основних типи VPN:

- VPN-брандмауер оснащений як брандмауером, так і VPN-можливостями. Цей тип використовує захист, надає малу кількість брендових аудіо, для обмеження доступу до внутрішніх мереж та забезпечує переведення адрес, автентифікацію користувача, аварійні сигнали та протоколювання.
- Апаратний VPN забезпечує високу пропускну здатність мережі та покращує продуктивність та надійність, але є дорогим.
- Програмне забезпечення VPN забезпечує гнучкість щодо управління трафіком. Це найкраще, коли кінцеві точки не контролюються однією стороною та при використанні різних брандмауерів та маршрутизаторів.
- (SSL) Secure Socket Layer VPN дозволяє користувачам підключатися до пристроїв VPN за допомогою веб-браузера. SSL використовується для шифрування трафіку між веб-браузером та пристроєм VPN.

Протоколи тунельного VPN пропонують різні функції та рівні захисту, і кожен має свої переваги та недоліки. Існує п’ять основних протоколів тунелювання VPN: протокол тунельного захисту Secure Socket (SSTP), протокол туннелювання Point-to-Point (PPTP), протокол тунелювання рівня другого (L2TP), OpenVPN та Інтернет-версія обміну ключами 2 (IKEv2).

- SSTP використовує протокол HTTPS для передачі трафіку через брандмауери та веб-проксі, які можуть блокувати інші протоколи. SSTP забезпечує механізм передачі трафіку протоколу PPP (point-to-point) через канал

SSL. Використання PPP дозволяє підтримувати сильні методи автентифікації, тоді як SSL забезпечує безпеку на транспортному рівні з розширеними переговорами щодо ключів, шифруванням та перевіркою цілісності.

- PPTP дозволяє шифрувати трафік декількох протоколів, а потім оберніть його в заголовок, який буде відправлений по мережі Інтернет-протоколу (IP). PPTP можна використовувати для віддаленого доступу та з'єднання VPN від точки до точки. Під час використання Інтернету сервер PPTP - це сервер VPN із підтримкою PPTP з одним інтерфейсом в Інтернеті та другим інтерфейсом у корпоративній інтрамережі. PPTP використовує з'єднання протоколу управління передачею для управління тунелем та загальної інкапсуляції маршрутизації для перенесення кадрів PPP для тунельованих даних.
- L2TP дозволяє шифрувати трафік з декількома протоколами, а потім використовувати будь-який носій, який підтримує доставку PPP, наприклад IP або асинхронний режим передачі. L2TP - це комбінація PPTP та пересилання рівня 2 (L2F). L2TP представляє найкращі можливості PPTP та L2F. На відміну від PPTP, L2TP покладається на захист IP (IPsec) у транспортному режимі для служб шифрування. Поєднання L2TP та IPsec відоме як L2TP / IPsec. L2TP і IPsec повинні підтримуватися як клієнтом VPN, так і сервером VPN. L2TP / IPsec - ідеальна пряма таємниця.
- OpenVPN - це програмний додаток з відкритим кодом, що реалізує методи VPN для створення безпечних з'єднань точка-точка або сайт-сайт у маршрутизованих або мостових конфігураціях та засобах віддаленого доступу. Він використовує власний протокол безпеки, який використовує SSL / TLS для обміну ключами. OpenVPN дозволяє партнерам перевіряти справжність один одного за допомогою закритого ключа, сертифікат або ім'я користувача і

пароль. Більшість постачальників VPN, що використовують OpenVPN, використовують пряму таємницю.

- IKEv2 - це протокол на основі IPSec, який використовується в Windows 7 і новіших версіях. IKEv2 - стандарт наступного покоління для безпечного обміну ключами між одноранговими мережами VPN. IKEv2 особливо корисний для автоматичного відновлення з'єднань VPN, коли користувачі тимчасово втрачають свої Інтернет-з'єднання.

Який найбезпечніший протокол VPN?

Незважаючи на те, що вони працюють із відкритим кодом, багато хто вважає OpenVPN найбезпечнішим протоколом VPN. Він стабільний і надійний, легко налаштовується для роботи на будь-якому порту, підтримує апаратне прискорення для підвищення швидкості, здатний обходити брандмауери та трансляцію мережевих адрес (NAT) і використовує бібліотеки OpenSSL для шифрування. Однак для цього потрібне клієнтське програмне забезпечення, і його не можна використовувати на iPhone і лише на обмеженій кількості телефонів Android.

Ще один захищений протокол - VPN-L2TP / IPSec. Він має потужний алгоритм шифрування, додаткове програмне забезпечення для пристроїв не потрібно, вбудований у більшість настільних операційних систем та мобільних пристроїв, досить простий у реалізації та не має відомих серйозних уразливостей. Однак він має проблеми з брандмауерами, його важче налаштувати на сервері Linux і відносно легко заблокувати провайдерами.

SSTP забезпечує надійне шифрування, його дуже важко виявити та заблокувати та підтримується на всіх пристроях Microsoft Windows. Однак він підтримується не всіма провайдерами VPN і має обмежену підтримку для пристроїв, що не належать до Windows [10].

Найменш безпечним протоколом VPN є PPTP. Його переваги включають просту настройку, широку підтримку більшості пристроїв та низькі накладні витрати. Оскільки він існує довгий час, йому відомі проблеми безпеки, якими можуть скористатися хакери (або державні установи). Він має слабке шифрування і його порівняно легко заблокувати провайдерами.

IKEv2 підтримується як частина реалізації Windows IPSec і простий у використанні. Однак помилки розробника все ще трапляються, а також існує проблема сумісності між різними постачальниками.

Який протокол VPN найкращий для підприємств та користувачів?

Для тих, хто шукає найбільш безпечний, OpenVPN може бути хорошим варіантом. Для тих, хто шукає підтримку багатьох пристроїв, PPTP може бути хорошим рішенням.

Висновки

1. Було розглянуто запобіжні заходи, які вживаються, щоб не допустити серйозних втрат користуючись віддаленим доступом.

2. Було розглянуто Використання технології VPN для забезпечення інформаційної безпеки.

VPN забезпечує доступ до захищеної корпоративної мережі через незахищені загальнодоступні мережі. Хоча VPN є покращенням у порівнянні з передачею незашифрованих даних через загальнодоступні мережі, користувачі, які планують розгортання VPN або вже використовують цю технологію, повинні враховувати потенційні недоліки безпеки. Використання VPN значно підвищує безпеку каналів зв'язку розподілених вузлів.

РОЗДІЛ 3
АНАЛІЗ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

3.1 Еволюція методів автентифікації від SFA до MFA

Постійне зростання кількості інтелектуальних пристроїв та відповідних навантажень на підключення має уражені мобільні послуги, які легко пропонуються в будь-якій точці земної кулі [11]. У такому пов'язаному світі, механізм захисту захищених переданих даних - це, насамперед, автентифікація.

Згідно з фундаментальною роботою в [12], автентифікація - це процес, коли “користувач ідентифікує себе сам, відправивши *x* в систему; система автентифікує його особу шляхом обчислення *F(x)* та перевіряючи, що воно дорівнює збереженому значенню y′′. Це визначення суттєво не змінилося з часом незважаючи на те, що простий пароль вже не є єдиним фактором для перевірки прав користувача [13].

Автентифікація залишається основним захистом від незаконного доступу до пристрою чи будь-якого іншого додатка, офлайн чи в режимі онлайн Рис. 3.1 Повернення в часі транзакцій були автентифіковані переважно за допомогою фізичної присутності, тобто, наприклад, шляхом нанесення воскової пломби [14].

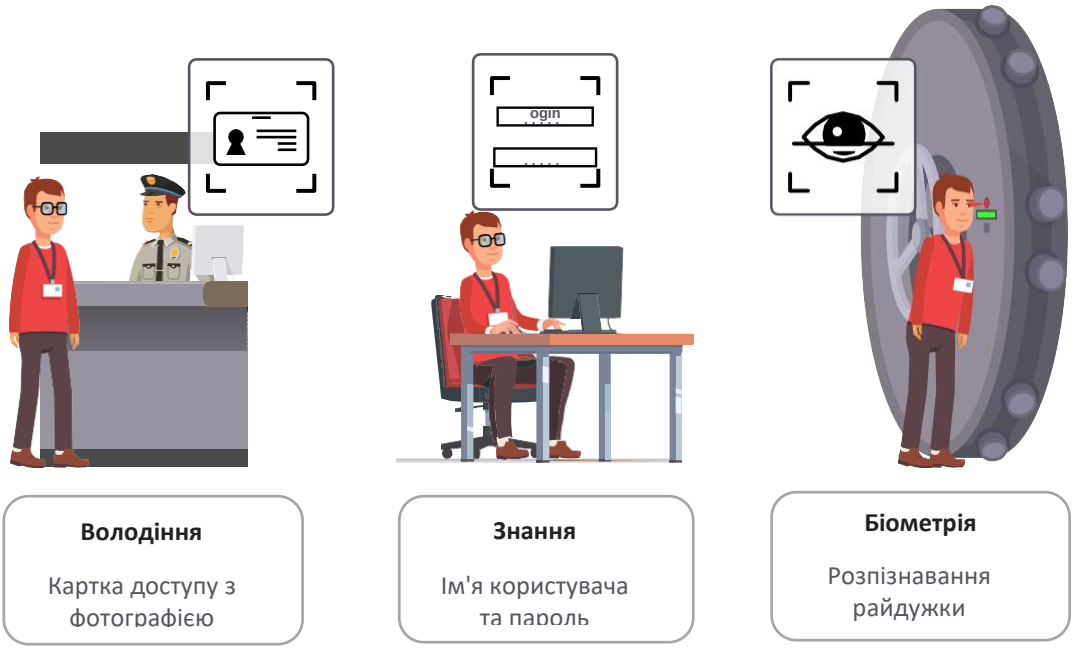


Рис. 3.1 Концептуальні приклади автентифікації.

Спочатку для автентифікації суб’єкта використовувався лише один фактор. На той час однофакторна автентифікація (SFA) в основному була прийнята спільнотою через її простоту та зручність для користувачів. Як приклад, можна розглянути використання пароля (або PIN-коду) для підтвердження права власності на ідентифікатор користувача. Мабуть, це найслабший рівень автентифікації. Поділившись паролем, можна негайно зламати обліковий запис. Більше того, несанкціонований користувач може також спробувати отримати доступ, використовуючи атаку за словником, таблицю веселки або техніки соціальної інженерії [15]. Зазвичай при використанні цього типу автентифікації слід враховувати мінімальну вимогу щодо складності пароля.

Крім того, було зрозуміло, що автентифікація лише за одним фактором не є надійною для забезпечення належного захисту через низку загроз безпеці [16].

Як інтуїтивний крок вперед було запропоновано двохфакторну автентифікацію (2FA), яка поєднує репрезентативні дані (комбінація ім’я користувача / пароль) із фактором особистого володіння, наприклад, смарт-карткою чи телефоном. Сьогодні доступні три типи факторних груп для зв’язку особи із встановленими даними:

1. *Фактор знань* - те, що користувач знає, наприклад, пароль або, просто, "секрет";

2. *Фактор власності* - те, що є у користувача, наприклад, картки, смартфони чи інші жетони;

3. *Біометричний фактор* - це те, що є користувачем, тобто біометричні дані або поведінка.

Згодом було запропоновано багатофакторну автентифікацію (MFA), щоб забезпечити більш високий рівень безпеки та полегшити постійний захист обчислювальних пристроїв, а також інших важливих служб від несанкціонованого доступу, використовуючи більше двох категорій облікових даних. Здебільшого MFA базується на біометрії, що є автоматизованим розпізнаванням людей на основі їх поведінкової та біологічних характеристик [17]. Цей крок забезпечив покращений рівень безпеки, оскільки користувачі повинні були представити докази своєї особистості, що спирається на два або більше різних факторів.

Обговорена еволюція методів автентифікації показана на Рис. 3.2.

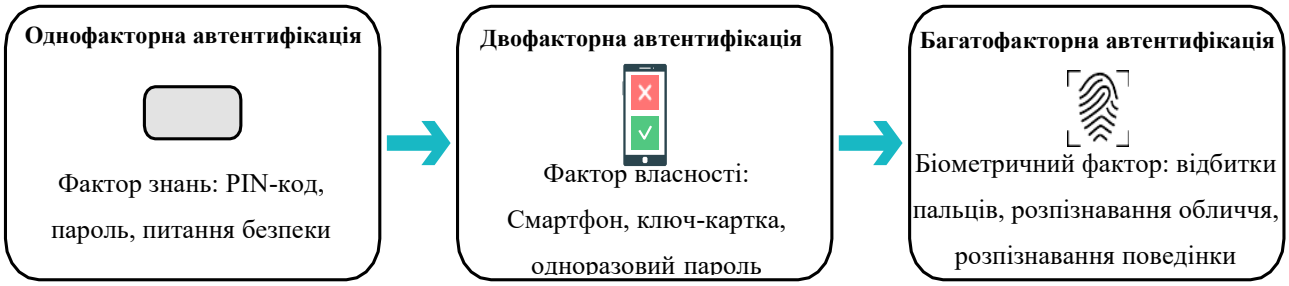


Рис.3.2 Еволюція методів автентифікації від SFA до MFA.

Сьогодні очікується, що MFA буде використовуватися в сценаріях, де вимоги безпеки вище, ніж зазвичай. За даними SC Media UK, 68 відсотків європейців готові використовувати біометричну автентифікацію для платежів. Розглянемо повсякденну практику зняття готівки в банкоматах. Тут користувач повинен надати фізичний токен (карту), що представляє фактор володіння, і підтримати його PIN-кодом, що представляє фактор знання, щоб мати можливість отримати доступ до особового рахунку і зняти гроші.

Як правило, додатки MFA можна розділити на три ринкові групи: (i) комерційні додатки, тобто вхід в обліковий запис, електронна комерція, банкомат, контроль фізичного доступу тощо; (ii) державні заявки, тобто документи, що засвідчують особу, державний документ, паспорт, водійські права, соціальне забезпечення, прикордонний контроль тощо; і (iii) судово-медичні програми, тобто кримінальне розслідування, пропажі дітей, ідентифікація трупів і т. д. Як правило, кількість сценаріїв, пов'язаних з автентифікацією, дійсно багато. Сьогодні MFA стає надзвичайно важливим фактором для:

- Підтвердження особистості користувача і електронного пристрою (або його системи);
- Перевірка підключення до інфраструктури;

- Перевірка взаємопов'язаних пристроїв IoT, таких як смартфон, планшет, або будь-який інший цифровий токен.

В даний час однією з основних проблем MFA є відсутність кореляції між ідентифікатором користувача і ідентифікаторами інтелектуальних датчиків в електронному пристрої / системі [18]. Що стосується безпеки, це ставлення має бути встановлено так, щоб тільки законний оператор, наприклад, той, чия особистість автентифікувати заздалегідь, міг отримати права доступу. У той же час процес MFA повинен бути максимально зручним для користувача, наприклад:

1. Клієнти спочатку реєструються і проходять автентифікацію у постачальника послуг, щоб активувати і управляти послугами, до яких вони хочуть отримати доступ;
2. Після отримання доступу до послуги користувач повинен пройти простий SFA з відбитком пальця / токеном, заздалегідь підписаним постачальником послуг;
3. Після початкового прийняття системою клієнт проходить автентифікацію, увійшовши в систему з тим же ім'ям користувача і паролем, які були встановлені раніше на клієнтському порталі (або в соціальній мережі). Для додаткової безпеки керуюча платформа може включати вторинні фактори автентифікації. Після того, як користувач успішно пройшов всі тести, фреймворк автоматично автентифікується на сервісній платформі;
4. Вторинна автентифікація відбувається автоматично на основі біометричного MFA, тому користувачеві буде запропоновано ввести додатковий код або надати токен-пароль тільки в разі збою MFA.

Біометрія дійсно робить значний внесок в схему MFA і може значно поліпшити перевірку особистості, поєднуючи фактор знання та мультимодальні

біометричними факторами, що значно ускладнює злочинцеві підслуховути системи, видаючи себе за іншу людину. Однак використання біологічних факторів має свої проблеми, в основному пов'язані з простотою використання, що в значній мірі впливає на зручність використання системи MFA.

З точки зору користувачів, сканер відбитків пальців вже забезпечує найбільш широко інтегрований біометричний інтерфейс. Це в основному пов'язано з тим, що його використовують на ринку виробники смартфонів. З іншого боку, його не рекомендується використовувати в якості автономного методу автентифікації. Однак використання будь-яких біометричних даних часто вимагає набору окремих сенсорних пристроїв. Використання вже інтегрованих дозволяє знизити витрати на систему автентифікації і полегшити впровадження кінцевими користувачами. Фундаментальний компроміс між зручністю використання і безпекою є одним з найважливіших чинників при розгляді систем автентифікації сьогодні [19].

Інша проблема полягає в тому, що використання біометрії гуртується на бінарному механізмі прийняття рішень [20]. Це було добре вивчено за останні десятиліття в класичній теорії статистичних рішень з точки зору автентифікації. Існують різні можливі рішення для контролю невеликої невідповідності фактичних «виміряних» біометричних даних і даних, що зберігаються в раніше захоплених зразках. Двома широко використовуваними методами є: коефіцієнт помилкового прийняття (FAR) [21] і коефіцієнт помилкового відхилення (FRR [22]. Маніпуляції з критеріями прийняття рішення дозволяють налаштувати структуру автентифікації на основі заздалегідь визначених витрат, ризиків і вигоди. Операція MFA сильно залежить від FAR і FRR, оскільки отримання нульових значень для обох показників практично неможливо. Оцінка більш ніж

однієї біометричної характеристики для встановлення особи людини може значно поліпшити роботу системи MFA.

3.2 Дослідження сучасних та потенційних джерел MFA

В даний час в системах автентифікації вже використовується величезна кількість датчиків, що дозволяють ідентифікувати користувача. У цьому розділі ми детально розглянемо чинники, які підходять для MFA, відповідні датчики, доступні на ринку, і пов'язані з цим проблеми. Крім того, ми надаємо додаткову інформацію про тих, які можуть бути розгорнуті в найближчому майбутньому.

Широко розгорнуті датчики / джерела MFA

Сьогодні ідентифікація і автентифікація для доступу до конфіденційних даних - один з основних варіантів використання MFA. Далі перераховуються чинники, вже доступні для використання MFA без придбання додаткового спеціалізованого обладнання.

1. Захист паролем

Звичайний спосіб автентифікації користувача - запит PIN-коду, пароля і т. д. [23]. Секретний пароль традиційно представляє фактор знання. Для автентифікації користувача потрібно тільки простий пристрій введення (принаймні, одна кнопка).

2. Токен

Потім пароль може бути доповнений фізичним токеном - наприклад, картою, яка рекомендується в якості другого фактора групи володіння. З апаратної точки зору користувач може уявити смарт-карту, телефон, переносний пристрій і т. д., які складніше делегувати [24].

У цьому випадку система повинна бути обладнана радіо інтерфейсом, що забезпечує двосторонній зв'язок з токеном. З іншого боку, найвідоміший програмний маркер - це одноразовий пароль, згенерований програмним

забезпеченням. Основним недоліком вищезазначеного чинника є проблема неконтрольованого дублювання.

3. Голосова біометрія

Більшість сучасних інтелектуальних електронних пристроїв оснащені мікрофоном, що дозволяє використовувати розпізнавання голосу як фактор для MFA [25]. У той же час, технологічний прогрес завтрашнього дня може дозволити спеціальним агенціям не лише розпізнавати мовців, але й імітувати їх голоси, включаючи інтонацію, тембр тощо, що є серйозним недоліком використання голосу як основного методу автентифікації.

4. Розпізнавання обличчя

Наступним кроком можна розглянути розпізнавання обличчя. На початку свого розвитку технологія базувалася на аналізі знакових зображень, яких було відносно просто відтворити, надавши системі фотографію [26]. Наступним етапом було надання можливості тривимірного розпізнавання обличчя, тобто прохання користувача рухати головою під час процесу автентифікації певним чином. Нарешті, прогрес цієї системи досяг точки визнання фактичних виразів користувача. Щоб забезпечити розпізнавання обличчя, потрібно оснастити систему принаймні одним вихідним пристроєм та камерою.

5. Окулярна методологія

Методи розпізнавання райдужної оболонки існують на ринку більше 20 років. Цей підхід не вимагає від користувача знаходитися близько до пристрою захоплення при аналізі колірного малюнка людського ока . Ще один привабливий метод - аналіз сітківки ока [27]. Тут захоплюється і аналізується тонка тканина, що складається з нервових клітин, які розташовані в задній частині ока. Аналіз сітківки є ще однією привабливою методикою [27]. Тут захоплюється і аналізується тонка тканина, що складається з нервових клітин,

розташованих у задній частині ока. Через складну будову капілярів, що постачають сітківку кров’ю, сітківка ока кожної людини унікальна. Найбільшими проблемами цих методів є необхідність у високоякісному пристрої зйомки та надійній математичній техніці для аналізу зображення.

6. Геометрія рук

Деякі системи використовують аналіз фізичної форми руки для автентифікації користувача. Спочатку для перевірки предмета використовувалися прив'язки, але такі методи використовувались не часто. Надалі планшетний сканер використовувався для отримання зображення без необхідності фіксувати руку користувача в одному конкретному положенні [28]. Сьогодні в деяких системах використовуються звичайні камери, які не потребують тісного контакту з поверхнею. Однак цей підхід не дуже стійкий до навколишнього середовища. Деякі виробники застосовують так звану *фотоплетізмографію* (PPG), щоб визначити, чи знаходиться переносний пристрій (наприклад, розумний годинник) в даний час на зап'ясті користувача чи ні. Цей процес аналогічний процесу вимірювання пульсу.

7. Розпізнавання вен

Досягнення сканерів відбитків пальців дають можливість також зібрати зображення вени пальця [29]. Більш складні пристрої використовують розпізнавання відбитків долоні, щоб придбати та зберегти форму / рух цілої руки. На сучасному етапі розвитку біометрія вен все ще вразлива до атак підміни.

8. Сканер відбитків пальців

Більшість постачальників смартфонів / персональних комп’ютерів в даний час використовують сканер відбитків пальців як основний механізм автентифікації. Це рішення є інтуїтивно зрозумілим у використанні, але залишається

надзвичайно простим у виготовленні - головним чином завдяки тому, що наші відбитки пальців можна отримати майже з будь-чого, до чого ми торкаємось. Інтеграційний потенціал цього методу справді високий, хоча його також не рекомендується використовувати як самостійний підхід до автентифікації. Більшість постачальників смартфонів встановлюють додаткову камеру для отримання відбитків пальців замість більш безпечного розпізнавання вен.

9. Теплове розпізнавання зображення

Подібно до розпізнавання вен, тепловий датчик використовується для реконструкції унікального теплового зображення потоку крові в тілі в безпосередній близькості. Багато проблем із цим методом автентифікації може виникнути через умови користувача: хвороба чи емоції можуть суттєво вплинути на сприйняті цифри.

10. Географічне розташування

Використання географічного положення пристрою і користувача для перевірки можливості надання доступу до пристрою / послузі є особливим випадком автентифікації на основі розташування. Важливо відзначити, що сигнал GPS може бути легко заблокований або вважатися несправним через властивості поширення; таким чином, рекомендується використовувати принаймні два джерела розташування, наприклад, GPS і ідентифікатор стільника бездротової мережі. Смартфон можна використовувати для підтримки MFA з точки зору визначення місця розташування.

Майбутнє інтеграції MFA

Прискорене впровадження у багатьох галузях, а також підвищення доступності біометричних послуг в широкому спектрі легкодоступних споживчих товарів підштовхують до концепції тісної інтеграції MFA. В даний

час дослідники і першопроходьці технологій намагаються інтегрувати нові датчики для використання в системах MFA.

1. Визначення поведінки

Свого часу функція розпізнавання поведінки використовувалася для аналізу ритму набору тексту військовим телеграфістом для відстеження пересування військ. Сьогодні жести для цілей автентифікації можуть варіюватися від звичайних до «важко імітованих», оскільки запрограмовані двигуном навички призводять до того, що рух організовується до фактичного виконання.

Сучасний приклад такої ідентифікації - це дотик до екрану смартфона. Цей підхід можна легко комбінувати з будь-якими методами автентифікації при введенні тексту, оскільки шаблон набору тексту унікальний для кожної людини. У разі, якщо система MFA спеціально розроблена для аналізу визначених жестів, від користувача вимагається відтворити раніше вивчене рух, утримуючи або надівши сенсорний пристрій.

Очевидним кроком автентифікації для широко використовуваних портативних і переносних пристроїв є використання відбитків пальців акселерометра. Наприклад, кожен власник смартфона може бути перевірений на основі моделі ходи шляхом безперервного моніторингу даних акселерометра, які практично неможливо підробити іншою людиною.

2. Техніка формування променя

З точки зору електрозв'язку, методи радіочастотної ідентифікації (RFID) і зв'язку ближнього поля (NFC) вже набули широкого поширення і визнання в суспільстві. Останні тенденції в області безпеки фізичного рівня стверджують, що використання бездротових рішень з множинним входом і безліччю виходів

(MIMO) для визначення місця розташування джерела сигналу може стати значним проривом в перевірці токена на тілі користувача.

3. Електрокардіографічне (ЕКГ) розпізнавання

Дані ЕКГ можна було зібрати з розумних годин користувача або трекера активності і порівняти з індивідуально збереженим зразком. Основна перевага використання цього фактора для автентифікації полягає в тому, що сигнали ЕКГ виступають в якості потенційного біометричного методу з тим перевагою, що їх важко (або майже неможливо) імітувати. Єдиний спосіб - використовувати існуючі особисті записи.

4. Електроенцефалографічне (ЕЕГ) розпізнавання

Це рішення засноване на аналізі мозкових хвиль і може розглядатися з фундаментального філософського положення «Cogito ergo sum» Р. Декарта або «Я думаю, отже, я існую». Це дозволяє отримати унікальний зразок патерну мозкової активності людини. Раніше реєстрацію даних ЕЕГ можна було виконувати тільки в клінічних умовах з використанням інвазійних зондів під черепом або електродів з вологим гелем, розташованих на шкірі черепа. Сьогодні простий збір ЕЕГ можливий з використанням доступних на ринку пристроїв, що мають розмір гарнітури.

5. Розпізнавання ДНК

Лінії клітин людини є важливим ресурсом для досліджень, які найбільш часто використовуються в зворотних генетичних підходах або в якості моделей захворювань людини in vitro. Це також джерело унікальної інформації про дактилоскопії ДНК. Незважаючи на те, що цей процес займає багато часу і є дорогим, він потенційно може використовуватися для попередньої авторизації користувача на високо захищених об'єктах поряд з іншими факторами.

На Табл. 3.1(а) та 3.1(б) наводиться порівняння основних показників для вже задіяних і виникаючих факторів. Фактори / датчики оцінюються на основі наступних параметрів:

- *Універсальність* означає наявність фактора в кожній людині;
- *Унікальність* вказує, наскільки добре фактор відрізняє одну людину від іншої;
- *Можливість збору* вимірює, наскільки легко отримати дані для обробки;
- *Продуктивність* вказує на досяжну точність, швидкість і надійність;
- *Прийнятність* означає ступінь прийняття технології людьми в їх повсякденному житті;
- *Підміна* вказує рівень складності захоплення і підробки зразка.

Таблиця 3.1(а) Порівняння відповідних факторів для MFA: В — високий; С — середній; Н — низький; н / д - недоступний.

Фактор	Універсальність	Унікальність	Можливість збору
Захист паролем	н / д	Н	В
Токен	н / д	С	В
Голосова біометрія	С	Н	С
Розпізнавання обличчя	В	Н	С
Окулярна методологія	В	В	С
Сканер відбитків пальців	С	В	С
Геометрія рук	С	С	С
Географічне розташування	н / д	Н	С
Розпізнавання вен	С	С	С
Теплове розпізнавання	В	В	Н

зображення			
Визначення поведінки	В	В	Н
Техніка формування променя	н / д	С	Н
ЕКГ	Н	В	Н
ЕЕГ	Н	В	Н
ДНК	В	В	Н

Таблиця 3.1(б) Порівняння відповідних факторів для MFA: В — високий; С — середній; Н — низький; н / д - недоступний.

Фактор	Продуктивність	Прийнятність	Підміна
Захист паролем	В	В	В
Токен	В	В	В
Голосова біометрія	Н	В	В
Розпізнавання обличчя	Н	В	С
Окулярна методологія	С	Н	В
Сканер відбитків пальців	В	С	В
Геометрія рук	С	С	С
Географічне розташування	В	С	В
Розпізнавання вен	С	С	С
Теплове розпізнавання зображення	С	В	В
Визначення поведінки	Н	Н	Н
Техніка формування променя	Н	Н	В
ЕКГ	С	С	Н
ЕЕГ	С	Н	Н
ДНК	В	Н	Н

Однак при інтеграції MFA для кінцевих користувачів необхідно вирішити багато інших проблем. У наступному розділі ми докладно розглянемо ці проблеми і формалізуємо рекомендації щодо спрощення інтеграції.

3.3 Дослідження проблеми операції MFA

Інтеграція нових рішень завжди була серйозною проблемою як для розробників, так і для менеджерів. Ключові проблеми представлені на Рис. 3.3. По-перше, прийняття користувачами є критичним аспектом для прийняття суворої ідентифікації і багатофакторної автентифікації. При прийнятті та розгортанні рішень MFA необхідно дотримуватися обережного і ретельного підходу, коли більшість проблем виникає з можливостей і потенційних вигод.

1. Зручність і простота

Основні проблеми зручності використання, що виникають в процесі автентифікації, можна охарактеризувати з трьох точок зору:

- Ефективність завдання - час на реєстрацію і час на автентифікацію в системі;
- Завдання спроби ефективності - номер входу для перевірки автентичності системи;
- Налаштування користувача - чи надає користувач перевагу певній схемі автентифікації перед іншою.

На додаток до підходів, що обговорювалися раніше, дослідники вже почали дослідження більш специфічних ефектів в процедурах автентифікації, заснованих на різних людських факторах. Автори провели дослідження того, як вік користувача впливає на ефективність завдання у випадках використання ПІН-коду і механізмів графічного доступу. Зроблено висновок, що молоде покоління може витрачати до 50 відсотків менше часу на проходження

процедури автентифікації в обох випадках. Цікаво, що автори показали, що стать в тому ж випадку не впливає на результати.

Інший підхід, що обговорювався раніше, дослідники вже почали дослідження більш специфічних ефектів в процедурах автентифікації, заснованих на різних людських факторах. Автори провели дослідження того, як вік користувача впливає на ефективність завдання у випадках використання ПІН-коду і механізмів графічного доступу. Зроблено висновок, що молоде покоління може витрачати до 50 відсотків менше часу на проходження процедури автентифікації в обох випадках. Цікаво, що автори показали, що стать в тому ж випадку не впливає на результати. Однак когнітивні відмінності між користувачами, тобто вербально або візуалізація, істотно впливають на виконання завдання.

Рис. 3.3 Основні операційні завдання MFA.

Крім того, важливу роль в цьому процесі відіграють властивості пристрою автентифікації. Автори досліджували можливість використання текстових паролів на мобільних пристроях. Було доведено, що використання смартфона або іншого обладнання без клавіатури для створення пароля має незадовільну зручність використання в порівнянні зі звичайними ПК.

Сьогодні більшість онлайн-сервісів автентифікації засновані на знаннях, тобто залежать від комбінації імені користувача та пароля. Більш складні системи вимагають, щоб користувач взаємодіяв з додатковими токенами (одноразові паролі, генератори коду, телефони і т. д.). Доповнюючи традиційні стратегії автентифікації, MFA неможливо без біометрії. З цієї точки зору в роботі [9] було проведено аналіз того, як гейміфікація і радість можуть позитивно вплинути на прийняття нових технологій. Проведене дослідження взаємодії з жестами показало, що безпека і взаємодія з користувачем не обов'язково повинні суперечити один одному. Ця робота також просувала задоволення як кращий спосіб швидкого впровадження технологій. У довідці розглядалася можливість використання рішення ЕКГ для автентифікації, і був зроблений висновок, що застосування ЕКГ ще не підходить для динамічного сценарію з реального життя.

Багато дослідників просували використання персональних портативних пристроїв під час процедури MFA. Michelin et al. запропонували використовувати камеру смартфона для лиця і райдужної оболонки визнання при збереженні прийняття рішень в хмарі. Інша робота по біометричній автентифікації для пристрою Android продемонструвала підвищений рівень задоволеності, пов'язаний з більш високою ефективністю завдань, досягнутої за допомогою рішення MFA. У якій вивчається зручність використання і практичність біометричної автентифікації на робочому місці. Був зроблений

висновок, що простота використання технології та її екологічний контекст грають життєву важливу роль - інтеграція і впровадження завжди спричинить за собою додаткові і несподівані витрати ресурсів.

Надзвичайно важлива проблема в зручності використання MFA полягає в тому, що «не всі користувачі можуть використовувати будь-яку задану біометричну систему». Люди, які втратили кінцівку в результаті аварії, можуть не пройти автентифікацію за відбитком пальця. Люди з ослабленим зором можуть зазнавати труднощів при використанні методів автентифікації на основі райдужної оболонки ока.

Біометрична автентифікація вимагає інтеграції нових послуг і пристроїв, що призводить до необхідності додаткової освіти під час усиновлення, що ускладняється для літніх людей і через пов'язаних з цим проблем зрозумілості. Зрозумілим є одне: досвід користувачів грає важливу роль в успішному впровадженні MFA; дехто каже: «користувач на першому місці». Сьогодні дослідження в області безпеки для автентифікації користувачів, заснованої на знаннях, знаходяться в процесі пошуку життєздатного компромісу між зручністю використання і безпекою - багато проблем ще не вирішені і незабаром з'являться.

Інтеграція

Навіть якщо всі проблеми зручності використання будуть вирішені на етапі розробки, інтеграція принесе додаткові проблеми як з технологічної, так і з людської точки зору.

Більшість споживчих рішень MFA залишаються апаратними. Як правило, «інтеграція фізичної та IT-безпеки може принести організації значні переваги, включаючи підвищення ефективності та відповідності вимогам, а також поліпшену безпеку». Однак збіжність не так проста. Пов'язані з цим проблеми

включають об'єднання груп фізичної та IT-безпеки, об'єднання компонентів різнорідних систем і оновлення систем фізичного доступу.

При розробці системи MFA слід ретельно враховувати незалежність біометричних даних. Необхідно забезпечити відповідність критеріям функціональної сумісності. Платформа повинна мати функціональні можливості для обробки біометричних даних з датчиків, відмінних від початку розгорнутих. Також слід враховувати використання мультибіометрії, тобто одночасне використання більш ніж одного фактора.

Ще одна серйозна проблема сумісності - це залежність від постачальника. Корпоративні рішення зазвичай розробляються як автономні ізольовані системи, які пропонують надзвичайно низький рівень гнучкості. Інтеграція недавно представлених на ринку датчиків потребують складних і дорогих оновлень, які, швидше за все, не будуть розглядатися найближчим часом.

Крім того, слід зазначити, що більшість доступних в даний час рішень MFA не мають повністю / частково відкритий вихідний код. Це ставить перед сторонніми постачальниками послуг питання про надійність і достовірність. При виборі структури MFA слід в першу чергу враховувати доступний рівень прозорості, що надається постачальниками обладнання і програмного забезпечення.

Безпека та конфіденційність

Будь-яка структура MFA - це цифрова система, що складається з критично важливих компонентів, таких як датчики, сховище даних, пристрої обробки і канали зв'язку. Всі вони зазвичай уразливі для безлічі атак на абсолютно різних рівнях, починаючи від спроб відтворення і закінчуючи атаками супротивника. Таким чином, безпека є необхідним інструментом для забезпечення і збереження конфіденційності. Тому почнемо з атак, які виконуються на самому

пристрої введення. Дозвіл доступу до конфіденційних персональних даних та їх обробки тільки законного контролера піддає співтовариство основними ризиками, пов'язаними з безпекою MFA, які перераховані нижче.

Перший з ключових ризиків пов'язаний з підробкою даних, яка буде успішно прийнята системою MFA. Примітно, що через те, що біометрія використовується різними структурами MFA, у зловмисника з'являється прекрасна можливість проаналізувати як технологію, що лежить в основі датчика, так і сам датчик, в результаті чого будуть виявлені найбільш підходящі матеріали для підробки. Основна мета архітекторів системи і устаткування - забезпечити або безпечне середовище, або, якщо це неможливо, заздалегідь розглянути відповідні можливості спуфинга. Ризик захоплення фізичних або електронних зразків і відтворення їх в системі MFA повинен бути ретельно усунутий.

Зазвичай для захисту від атак з електронним відтворенням потрібне використання мітки часу. На жаль, виконати атаку з використанням біометричного спуфинга досить просто. Незважаючи на те, що біометрія може поліпшити продуктивність системи MFA, вони також можуть збільшити кількість вразливостей, які можуть бути використані зловмисником. Додатковим ризиком є крадіжка конфіденційних даних під час передачі між датчиком і блоком обробки / зберігання. Така крадіжка може в першу чергу відбуватися через небезпечне передавання від пристрою введення через вилучення та зіставлення блоків в базі даних, і існує ймовірність атаки. Повинен бути гарантований необхідний рівень безпеки даних, щоб протистояти цьому типу ризику.

Ще одна можливість атакувати систему MFA - це захоплення вибірки секретних даних. Що стосується факторів знання, система буде негайно

скомпрометована, якщо не будуть використовуватися рішення з нульовим розголошенням. Особливий інтерес представляє одержання біометричного зразка, який неможливо відновити або змінити з плином часу. Отже, захист біометричних даних вимагає більш високого рівня безпеки на етапах збору, передачі, зберігання і обробки [30].

Наступний ризик пов'язаний з крадіжкою зі сховища даних. Зазвичай бази даних зберігаються централізовано, що забезпечує єдину точку відмови. У той же час деякі з віддалених систем, що контактують з базою даних, не завжди мають законні права на доступ до збережених особистих даних. Для захисту даних від крадіжки потрібен високий рівень ізоляції на додаток до використання необоротного шифрування [31]. Наступний ризик пов'язаний з атаками, пов'язаними з місцем розташування. Сигнал GPS може бути уразливий для блокування місця розташування (перешкоди) або подачі неправдивої інформації в приймач, щоб він обчислював помилковий час або місце розташування (підміна). Аналогічні методи можуть бути застосовані до послуг визначення розташування на основі стільникового зв'язку і WLAN [32,33].

Нарешті, будучи системою інформаційних технологій, структура MFA повинна забезпечувати відносно високі рівні «пропускної спроможності», що відображає здатність системи задовольняти потреби своїх користувачів з точки зору кількості спроб введення за період часу. Навіть якщо біометрія вважається підходящою у всіх інших аспектах, але система може виконувати тільки, наприклад, одне зіставлення на основі біометричних даних в годину, в той час як потрібно працювати зі швидкістю 100 зразків на годину, таке рішення не слід розглядати як здійсненне. Тут рекомендується вибрати відповідне обладнання для обробки даних для сторони сервера / захоплення.

Структура безпеки MFA повинна також підтримувати панель тестування на проникнення для оцінки її потенційних слабких місць. Сьогодні розробники часто проводять зовнішній аудит для оцінки ризиків і діють на основі такої оцінки для більш ретельного планування. Таким чином, слід оцінити систему MFA для забезпечення більш безпечного середовища.

Надійність до робочого середовища

Навіть якщо питання безпеки і конфіденційності будуть повністю вирішені, біометричні системи, в основному дактилоскопічні, не відповідали вимогі «надійності» з самого початку свого шляху [34]. В основному це відбулося через те, що експлуатаційні випробування проводилися в лабораторних умовах, а не в польових умовах. Одним з яскравих прикладів є розпізнавання голосу, яке було дуже надійним в тихій кімнаті, але не могло підтвердити користувача в міських умовах.

Аналогічна проблема відноситься до методів раннього розпізнавання осіб, які не працювали без адекватної світловий підтримки, якісної камери і т.д. Зворотною стороною медалі була необхідність постійного спостереження за піддослідним. Навіть сьогодні є або поради про те, де дивитися / класти пальці, або наочні посібники під час перевірки безпеки. Відсутність досвіду взаємодії між машинами і людьми зазвичай аналізується за допомогою показників «Відмова від реєстрації» (FTE), а також «Відмова від набору» (FTA) [35]. Обидва вони залежать від самих користувачів, а також від додаткового шуму навколишнього середовища.

Оскільки значна частина MFA сильно залежить від біометрії, вона може бути класифікована як імовірнісна за своєю природою. Основа біометричної автентифікації лежить в області зіставлення зі зразком, яке, в свою чергу, базується на наближенні. Приблизне узгодження є важливим аспектом в будь-

якій системі MFA, оскільки різниця між користувачами може мати вирішальне значення через безліч факторів і невизначеності. Зображення, отримане під час сканування відбитку пальця, буде відрізнятися кожен раз, коли воно буде спостерігатися через кут огляду, тиску, бруду, вологості або відмінностей датчиків, навіть якщо воно знято одною і той же людиною.

Для кількісної оцінки ефективності системи біометричної автентифікації використовуються два важливих коефіцієнта помилок: FAR і FRR. FAR - це відсоток самозванців, яких помилково допустили в якості справжніх користувачів. Він визначається як відношення кількості помилкових збігів до загальної кількості спроб зіставлення самозванців. FRR - це кількість справжніх користувачів, яким відмовлено у використанні системи, яке визначається як відношення кількості помилкових відмов до загальної кількості спроб справжнього зіставлення.

В літературі також рекомендується використовувати коефіцієнт помилок кросовера (CER) на додаток до раніше обговорених метрик. Цей параметр визначається як ймовірність того, що система знаходиться в стані, в якому FAR рівне FRR. Чим нижче це значення, тим краще працює система. Відповідно до цього, «вищий FAR кращий в системах, де безпека не має першорядного значення, тоді як більш високий FRR краще в додатках з високим рівнем безпеки». Точка рівності між FAR і FRR називається рівною частотою помилок (EER). На підставі вищевикладеного можна ще раз зробити висновок, що система, яка використовує виключно біометричні дані, не може вважатися кращою структурою MFA.

Аналізуючи перераховані вище проблеми, можна оцінити всю систему MFA. Далі запропоновано підхід, що дозволяє використовувати MFA, заснований на наявності великої кількості датчиків.

Висновки

1. Була розглянута еволюція методів автентифікації від SFA до MFA.
2. Були досліджені сучасні та потенційні джерела MFA, розглянуті чинники, які підходять для MFA, відповідні датчики, доступні на ринку, і пов'язані з цим проблеми.
3. Розглянуті ключові ризики пов'язані з підробкою даних , які будуть успішно прийняті системою MFA.
4. Були досліджені інтеграції нових послуг і пристроїв.

РОЗДІЛ 4

МЕТОД ПІДВИЩЕННЯ РІВНЯ ОЦІНКИ БЕЗПЕКИ АБОНЕНСЬКОГО З'ЄДНАННЯ ПРИ ОРГАНІЗАЦІЇ ВІДДАЛЕНОГО ДОСТУПУ.

Зазвичай у користувача є ім'я користувача / пароль / ПІН / токен, і його додатково попросять використовувати біометричний фактор, такий як риси обличчя або відбитки пальців. Якщо процедура автентифікації не може встановити довіру за допомогою цієї комбінації чинників, то користувачеві буде запропоновано пройти автентифікацію з використанням іншого раніше зареєстрованого фактору або їх набору. Ця система MFA може не тільки перевіряти точність призначеного для користувача введення, але також визначати, як користувач взаємодіє з пристроями, тобто аналізувати поведінку. Чим більше користувач взаємодіє з біометричної системою, тим точніше стає її робота.

Ще одна особливість обговорюваного сценарію - це фактична зручність використання датчика. Якщо використовується датчик (наприклад, пристрій для читання відбитків пальців), і цей пристрій недоступно з того місця, де користувач намагається увійти в систему або отримати доступ, призначений для користувача досвід стає неадекватним. Наявність пристрою подвійного призначення - смартфона або розумних годин (підходять для виконання примітивів інформаційної безпеки), яке користувач вже має в своєму розпорядженні - як додатковий фактор MFA (не тільки в якості токена) робить систему вартість і зручність використання набагато розумніше.

Наявність великої кількості сенсорних даних підводить нас до наступного логічного етапу їх застосування в MFA. Ми також припускаємо можливе використання відповідних факторів для автентифікації користувача без

використання спеціального «верифікатора» з фактичними біометричними даними, за винятком даних, зібраних у реальному часі.

4.1. Опис підходу заснованого на використані поліномів Лагранжа

Один з підходів, розглянутих в рамках даної роботи, заснований на використанні поліномів Лагранжа для поділу секрету. Системний секрет S зазвичай «розділяється» між набором власників ключів. Його можна буде відновити пізніше, як описано в [35] і багатьох інших роботах, наприклад,

$$f(x) = S + a_1 x + a_2 x^2 + \cdots + a_{l-1} x^{l-1},$$
$$f(0) = S, \tag{4.1}$$

де a_i - згенеровано поліноміальні індекси, а x - унікальний фактор ідентифікації F_i. У таких системах кожен держатель ключа з ідентифікатором фактора отримує свій власний унікальний загальний ключ $S_{ID} = f(ID)$.

У звичайних системах потрібно зібрати будь-які l часткою $\{S_{ID_1}, S_{ID_1}, \cdots, S_{ID_l}\}$ початкового секрету для розблокування системи, в той час як крива може пропонувати $n > l$ точок, як показано на Рис.4.1. Базовий принцип цього підходу полягає у вказівці секрету S і використанні згенеровано кривої на основі випадкових коефіцієнтів a_i для отримання секретних частин S_i. Ця методологія успішно використовується в багатьох системах спільного використання секретів, в яких використовується формула інтерполяції Лагранжа.

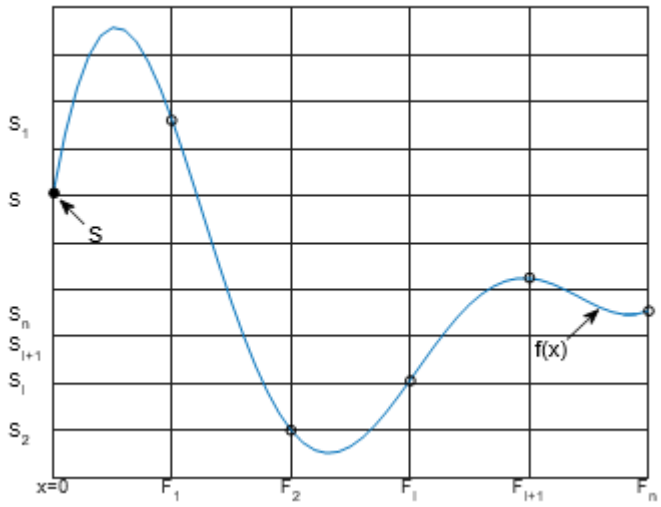


Рис.4.1 Схема секретного обміну Лагранжа.

На жаль, цей підхід не може бути застосований для сценарію MFA безпосередньо [36], оскільки біометричні параметри вже встановлені, тобто ми не можемо ні призначити новий S_i користувачеві, ні змінити їх. З одного боку, користувач може встановити деякі особисті чинники, такі як пароль, PIN-код і т. д. З іншого боку, деякі з них можуть бути незмінними (біометричні параметри і атрибути поведінки). В цьому випадку повинна бути вирішена зворотна задача, в якій частки секретного S_{ID_i} відомі як значення факторів S_i. В основному S_i фіксуються і стають унікальними $\{S_{ID_1,}S_{ID_1},\cdots,S_{ID_l}\}$ при установці для користувача. У цьому випадку S є секретом для доступу до системи і повинен бути отриманий зі значеннями фактору користувача. Можливе рішення, засноване за оберненою формулою інтерполяції Лагранжа, пропонується в наступному підрозділі.

4.2. Запропонована зворотна методологія, заснована на поліномі Лагранжа

У цій роботі було розглянуто систему MFA з явними l факторами F. Кожен фактор F_i має унікальний секрет S_i, отриманий за допомогою відповідної процедури (PIN, відбитки пальців і т. д.) від користувача. У гіршому випадку це пов'язано з біометричними даними - ймовірність того, що вони з часом зміняться, мала. Потім відповідні фактори та секрети можуть бути представлені як

$$\begin{aligned} F_1 &: S_1, \\ F_2 &: S_2, \\ &\cdots \\ F_l &: S_L, \\ F_{l+1} &: T, \end{aligned} \tag{4.2}$$

де S_i - значення секрету, отримане від датчика (коефіцієнта), l - кількість факторів, необхідних для відновлення секрету, а $F_l + 1$ - мітка часу, зібрана в момент часу T.

Важливо відзначити, що для надання фактичних секретів верифікатори не є варіантом, особливо в разі конфіденційних біометричних даних, тому що відбиток пальця зазвичай є незмінним фактором. Отже, дозволити навіть довіреному примірнику отримати відповідні дані - сумнівний крок. І навпаки, в порівнянні з методом, розглянутим в розділі 4.1, модифікований алгоритм має на увазі, що S_i виходять з факторів (тільки один поліном описує відповідну криву), як показано на Рис.4.2. Іншими словами, запропонована методологія створює систему, де S секрет на основі зібраних значень факторів S_i, замість того, щоб призначати їх в першу чергу.

Система рівнянь, пов'язана з інтерполяційною формулою Лагранжа, з факторами, їх значень і секретом доступу до системи

$$\begin{cases} S_1 = \bar{S} + a_1 F_1 + a_2 F_1^2 + \cdots + a_{l-1} F^{l-1} + a_1 F_1^l, \\ S_2 = \bar{S} + a_1 F_2 + a_2 F_2^2 + \cdots + a_{l-1} F^{l-1} + a_1 F_2^l, \\ \cdots \\ S_1 = \bar{S} + a_1 F_1 + a_2 F_1^2 + \cdots + a_{l-1} F^{l-1} + a_1 F_l^l, \\ T = \bar{S} + a_1 T + a_2 T^2 + \cdots + a_{l-1} T^{l-1} + a_1 T^l, \end{cases} \tag{4.3}$$

де a_i - відповідні згенеровані коефіцієнти, $f(x) = S + a_1 x + a_2 x^2 + \cdots + a_{l-1} x^{l-1}$, та $f(0) = S$. Система в рівнянні (3) має тільки одне рішення для *S*, і воно добре відомо з формули інтерполяції Лагранжа.

Лемма 1. *Одна і тільки одна поліноміальна крива f (x)* ступеня $l - 1$ *можна описати l точками на площині* $(x_1, y_1), (x_2, y_2), \ldots, (x_l, y_l)$

$$f_x = a_0 + a_1 x + \cdots + a_{l-1} x^{l-1}, \{f(x_i) = y_i\}_{i=1.}^{l} \tag{4.4}$$

Отже, системний секрет *S* може бути відновлений на основі *l* зібраних часткою, заданих традиційною формулою інтерполяції Лагранжа, без необхідності передавати вихідні секрети факторів S_i верифікатори. Отже, конфіденційні персональні дані залишаються конфіденційними, оскільки

$$S = (-1)^l \sum_{i=1}^{l+1} S_i \prod_{j=1, j \neq i}^{l+1} \frac{F_j}{F_i + F_j}, \tag{4.5}$$

де $F_{l+1} = T$. Запропоновані модифікації необхідні для забезпечення унікальності отриманих даних, зображено на Рис.4.2.

В силу властивостей формулювання Лагранжа може бути тільки одна крива, описувана відповідним многочленом (Лемма 1); отже, кожен набір [F_i: S_i] створить свій унікальний S.

Однак, якщо біометричні дані, зібрані MFA, не змінювалися з плином часу, секрет завжди залишиться колишнім, що є очевидною вразливістю даної системи. З іншого боку, просте додавання мітки часу завжди має давати унікальну криву, як це показано на Рис.4.2 для T, T_1 та T_2.

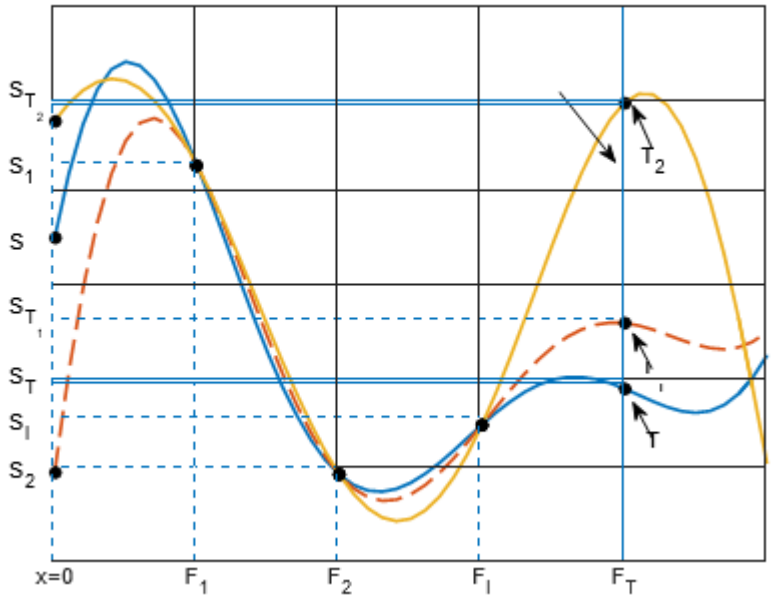


Рис.4.2 Зворотний метод, заснований на поліномі Лагранжа.

Пропоноване рішення забезпечує стійкість до випадку, де всі S_i залишається незмінним з часом. Це досягається за рахунок додавання унікального фактору часу T, який робить можливим присутність F_l з відповідним секретом.

Необхідно відзначити, що розглянута порогова схема, заснована на формулі інтерполяції Лагранжа, використовує механізм Ривеста - Шаміра

Адлемана (RSA) або алгоритм шифрування / дешифрування Ель-Гамаля для автентифікації на заключному етапі. В цьому випадку доведено, що ми отримуємо безпечну порогову схему, яка відноситься до секретів S_i в [214].

4.3. Запропоноване рішення MFA

Дійсно, запропоноване рішення може працювати «з коробки» в разі, якщо присутні всі l фактори. Таким чином, система може запропонувати можливість ідентифікувати та повідомити будь-яку застарілу інформацію про фактори, наприклад, коливання ваги. Доступ до послуги можна автоматизувати за відсутності деяких факторів. Більш детально розглянемо цю функцію в поточному підрозділі.

Фактор невідповідності

Якщо припустити, що кількість факторів в нашій системі $l = 4$, секрет системи S може бути представлений в спрощеному вигляді як група

$$S \leftarrow [F_1\ F_2\ F_3\ F_4] \tag{4.6}$$

Тут, якщо який-небудь з S_i буде змінений - механізм відновлення секрету вийде з ладу. Поліпшення цього алгоритму досягається шляхом надання окремих системних рішень S_i для меншої кількості зібраних факторів.

В основному, для $l = 3$ кількість можливих комбінацій факторів з одним пропущеним дорівнює чотирьом, в такий спосіб

$$\begin{aligned} \overline{S_1} &\leftarrow [F_1\ F_2\ F_3], \\ \overline{S_2} &\leftarrow [F_1\ F_3\ F_4], \\ \overline{S_3} &\leftarrow [F_1\ F_2\ F_4], \\ \overline{S_4} &\leftarrow [F_2\ F_3\ F_4]. \end{aligned} \tag{4.7}$$

Таким чином, пристрій може надавати доступ на основі заздалегідь визначеної політики функції ризику. В якості другої переваги він може інформувати користувача (або повноважний орган) про те, що конкретний фактор F_i повинен бути оновлений на основі невдалої комбінації S_i. Дійсно, ця модифікація приносить лише незначні накладні витрати на передачу, але, з іншого боку, забезпечує більш високу гнучкість в автентифікації і перевірки відсутнього фактору.

Хмарна допомога

Ще один важливий сценарій для MFA - потенційна допомога довіреного органу в $F_i : S_i$. У разі, коли користувач не може уявити достатню кількість факторів, довірений орган може записувати дані про тимчасові ключові фактори, як показано на Рис.4.3.

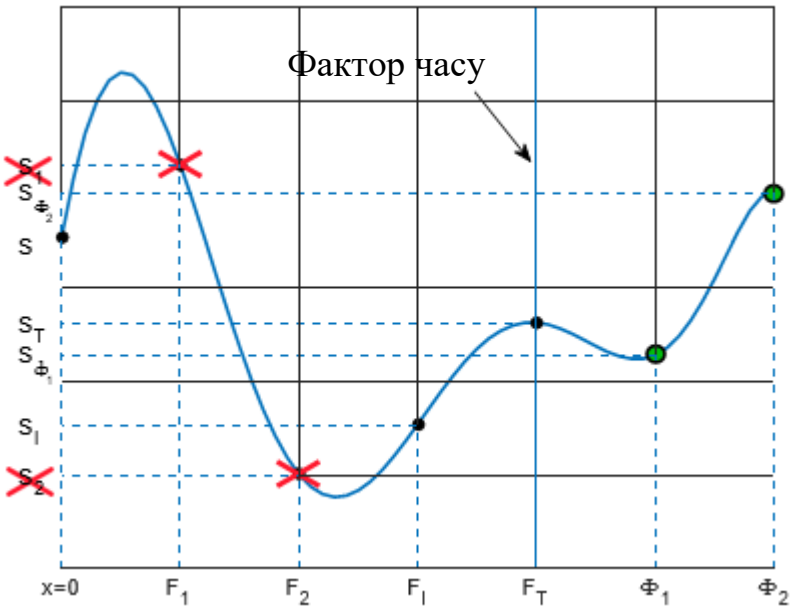


Рис.4.3 Допомога довіреним органам в автентифікації, коли користувач не має двох факторів.

Наприклад, припустимо, що користувач забув або втратив два фактори F_2 та F_3 з відповідними ключами $S_1 = f(F_1)$ та $S_2 = f(F_2)$. Довірений орган готовий допомогти в автентифікації - таким чином, генеруються два тимчасових ключа $S_{\Phi_1} = f(\Phi_1)$ та $S_{\Phi_2} = f(\Phi_2)$, які відправляються користувачеві через захищений канал. Отримання цих ключів і застосування формули інтерполяції Лагранжа з процедурою порогової автентифікації на основі шифрування / дешифрування RSA або Ель-Гамаля включає наступні чинники і ключі

$$\begin{gathered} F_1 : S_1, \\ F_2 : S_2, \\ \ldots \\ F_l : S_L, \\ F_{l+1} : T, \\ \Phi_1 : S_{\Phi_1}, \\ \Phi_2 : S_{\Phi_2}, \end{gathered} \tag{4.8}$$

як описано в [27]. Це дозволяє отримати доступ до пристрою.

Пропоноване рішення спеціально розроблено для завершення етапу автентифікації MFA, тобто його використання для SFA і 2FA не рекомендується. В основному це пов'язано з особливостями формули інтерполяції Лагранжа. В принципі, в разі SFA і без фактору $F_{l+1} : T$ дане рівняння можна просто уявити як $S_1 = S + b_1 F_1$, тобто воно стане «точкою». Навіть додавання випадкового фактору тимчасової мітки не забезпечить будь-якого цінного рівня захисту біометричних даних, так як перехоплювач може негайно відновити секрет фактору.

Вищезазначене також не підходить для 2FA, оскільки надання двох факторів дозволяє кривій мати лінійну поведінку, тобто перехоплювачу

потрібно дві спроби відновити пароль. Однак додавання фактору тимчасової мітки дозволяє забезпечити необхідний рівень безпеки з трьома фактичними факторами, як описано нижче.

4.4 Вдосконалений метод оцінки рівня безпеки абонентського з'єднання

Зазвичай системи автентифікації, що використовують тільки інформацію про фактори володіння, працюють в режимі придатний / непридатний, тобто вхідні дані або вірні, або невірні. Коли справа доходить до використання біометрії, система стикається з потенційними помилками під час збору біометричних зразків, що обговорювалося раніше в розділі 3. Далі продовжуємо розвивати запропоновану методологію з критичної точки зору FAR / FRR.

Зазвичай параметри FAR / FRR датчика надаються постачальниками на основі статистично зібраних даних [28]. Для структури MFA ми припускаємо, що на етапі автентифікації користувача будуть прийняті два можливих рішення, як показано на Рис.4.4: (i) H_0 - користувач не є легітимним; або (ii) H_1 - користувач є законним. Вони утворюють весь простір вибірки $\mathrm{P}(H_0) + P(H_1) = 1$. Передбачається, що політикою ризику займається власник системи автентифікації, який також встановлює розподіли $P(H_0)$ і $P(H_1)$.

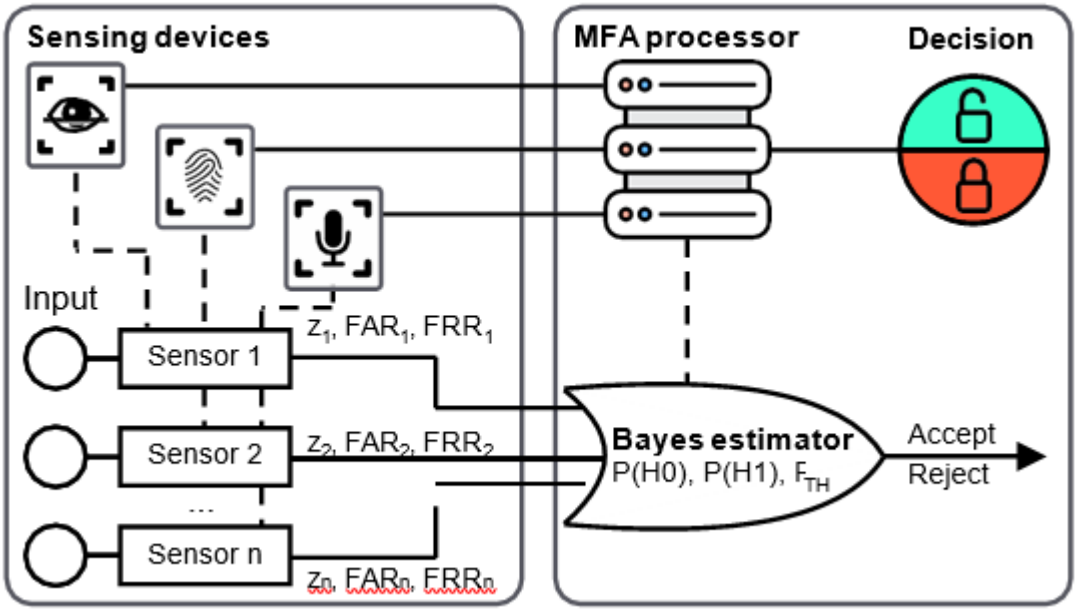


Рис.4.4 Системний режим MFA. PTH - вибраний поріг.

Загалом, може бути n біометричних датчиків, що збирають дані, що вводяться користувачем. Вимірювання кожного окремого датчика з набору $Z = \{z_1, \dots, z\}$ розподіляється в межах *[0, 1]*, і ця множина далі аналізується в умовах двох раніше розглянутих гіпотез. Вимірювання, отримані від датчиків, можна було обробляти двома різними способами, як описано в продовженні.

Методологія суворих рішень

Кожен датчик вирішує, чи є користувач законним чи ні, повертаючи accept або reject. Потім система MFA об'єднує зібрані результати і надає групове рішення на основі отриманого вектору. Отже, можна використовувати функції порогового рішення або зважені граничні функції в залежності від надійності датчика.

У першому випадку датчик поверне значення z_i, $z_i = [0; 1]$, що можна інтерпретувати як ТАК чи НІ. Тоді умовні ймовірності $P(z_i \mid H_0)$ і $P\ (z_i \mid H_1)$ визначаються значеннями *FARi* та *FRRi*, відповідно, для *i*-го датчика. Тут *FARi* і

FRRi беруться в точці CER / EER, наприклад, z_i вибирається в точці, де *FARi* = *FRRi*. Як правило, ця методологія відображає сценарії володіння або факторів знань з біометричної точки зору.

Методологія імовірнісних рішень

Датчик реагує результатом своїх вимірів, а також ймовірнісними характеристиками. Далі дані об'єднуються до прийняття остаточного рішення. Отже, весь набір даних вимірювань може використовуватися при прийнятті групового рішення і, відповідно, загальний результат може бути встановлений на основі набору, отриманого від усіх датчиків.

У другому випадку датчик повертає результат вимірювань, а також порівняння шаблонів у вигляді оцінки збігу z_i $(0 \leq z_i \leq 1)$. Для кожного із значень z_i умовна ймовірність $P(z_i | H_0)$ обчислюється на основі значень *FARi* в точці z_i. Крім того, умовна ймовірність $P(z_i | H_1)$ визначається значеннями *FRRi* в z_i.

Такий підхід дає можливість розглядати методологію строгих рішень як спрощену модель ймовірності для випадку, коли *FARi* та *FRRi* задані тільки в одній точці. Тут результат вимірювання може приймати тільки два значення, тобто вище або нижче обраного порога.

Оцінка

У цій роботі розглядається більш загальний випадок імовірнісної методології прийняття рішень, в той час як комбінація результатів вимірювань для окремих датчиків проводиться аналогічно попереднім роботам з використанням Байківської оцінки [39]. Оскільки результати вимірювань мають ймовірнісний характер, вирішальна функція підходить для вирішення з максимально апостеріорною ймовірністю.

Більш докладно функція прийняття рішення може бути описана наступним чином. На вході потрібна умовна ймовірність виміряного значення від кожного датчика $P\ (z_i \mid H_0)$ та $P\ (z_i \mid H_1)$ разом з апріорними ймовірностями гіпотез $P\ (H_0)$ та $P\ (H_1)$. Останні значення можуть бути частиною політики компанії по відношенню до ризиків, оскільки вони визначають ступінь довіри для конкретних користувачів. Потім функція прийняття рішення оцінює апостеріорну ймовірність гіпотези $P\ (H_1 \mid Z)$ і перевіряє, що відповідна ймовірність вище заданого порогового значення P_{TH}.

Умовні ймовірності, пов'язані з вимірами, можна розглядати як незалежні випадкові величини; отже, загальна умовна ймовірність така:

$$P\left(Z\middle|H_j\right) = \prod_{z_i \epsilon\ Z} P(z_i \mid H_j), J \in \{0; 1\}. \tag{4.9}$$

Далі, повна ймовірність *P (Z)* обчислюється як

$$P(Z) = \prod_{z_i \in Z} P(z_i \mid H_0)P(H_0) + \prod_{z_i \epsilon\ Z} P(z_i \mid H_1)P(H_1), \tag{4.10}$$

де $P\left(z_i\middle|H_j\right), J \in \{0; 1\}$ відомі з характеристик датчиків, а $P(H_0)$ і $P\ (H_1)$ - апріорні ймовірності гіпотез (частина політики компанії щодо ризиків).

На підставі отриманих результатів апостеріорна ймовірність для кожної гіпотези HJ , *J ∈{0; 1}* можуть бути виготовлені.

$$P(H_1|Z) = \frac{\prod_{z_i\,\epsilon\,Z} P(z_i|H_1)P(H_1)}{P(Z)}. \tag{4.11}$$

Для комплексного вирішення по всьому набору датчиків застосовується наступне правило

$$P(H_1|Z) > P_{TH} \Longrightarrow \{Accept\}, else\ \{Reject\}. \quad (4.12)$$

В результаті рішення може бути правильним або призвести до помилки. Потім значення FAR та FRR можуть бути використані для вибору відповідного порогу PTH на основі всіх задіяних сенсорів.

4.5 Обговорення та перспективи на майбутнє.

Сьогодні автентифікація важлива як ніколи раніше. У цифрову епоху більшість користувачів будуть покладатися на біометрії в питаннях, що стосуються безпеки систем і авторизації, на додаток до звичайних паролів. Незважаючи на те, що проблеми з конфіденційністю, безпекою, зручністю використання і точністю все ще зберігаються, MFA стає системою, яка обіцяє безпеку і простоту використання, необхідні для сучасних користувачів при отриманні доступу до конфіденційних даних.

Без сумніву, біометрія - один з ключових рівнів, що забезпечують майбутнє MFA. Ця функція часто розглядається не як окрема, а як доповнення до традиційних підходів до автентифікації, таким як паролі, смарт-карти і PIN-коди. Очікується, що об'єднання двох або більше механізмів автентифікації забезпечить більш високий рівень безпеки при перевірці користувача. Очікувана еволюція в бік MFA заснована на синергетичних біометричних системах, які дозволяють значно поліпшити взаємодію з користувачем і пропускну здатність системи MFA, що буде корисно для різних додатків (див. Рис.4.5). Такі системи розумно об'єднають всі три типи факторів, а саме знання, біометрії і володіння.

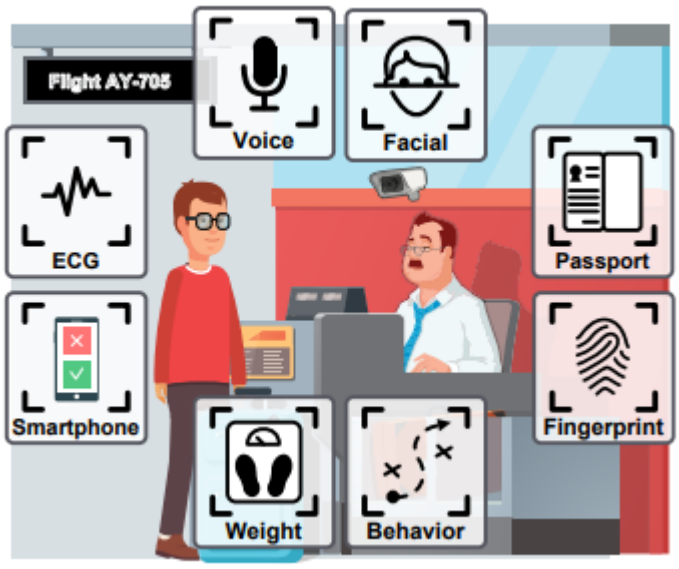


Рис.4.5 Біометричний MFA для сценарію аеропорту.

Оскільки сучасні однофакторні системи засновані тільки на одному параметрі (властивості унімодальності), якщо на його одержання будь-яким чином вплине (будь то шум або збої), загальна точність знизиться. Нагадуємо, що збір одного типу даних, які пов'язані зі знаннями, наприклад, біометричних даних, може виключити частину користувачів при наявності певних порушень. Більш того, спуфинг цього єдиного чинника - відносно просте завдання.

Одним з найбільш багатообіцяючих напрямків в MFA є біометрія на основі поведінки, що забезпечує абсолютно нові способи автентифікації користувачів. Рішення, засновані на м'язовій пам'яті, наприклад листі або жестах, в поєднанні з машинним навчанням стають більш яскравими прикладами. Уже сьогодні програмне забезпечення може екстраполювати почерк користувача і досягати рівня достовірності вище 99,97%. Більш перспективними джерелами MFA, які будуть використовуватися в найближчому

майбутньому, є серце і мозок. Очікується, що приваблива область аналізу ЕКГ і ЕЕГ наддасть унікальні ідентифікаційні зразки для кожного суб'єкта.

Інше дослідження, натхнене військовими, вже демонструє здатність ідентифікувати користувачів по тому, як вони взаємодіють з комп'ютером. Цей підхід враховує швидкість набору тексту, типові орфографічні помилки, ритм листи та інші фактори. Відповідна термінологія ще не визначена, і деякі називають цю методологію пасивною біометрією, а інші називають її безперервною автентифікацією. В результаті виходить унікальний відбиток моделі взаємодії користувача з комп'ютером, який надзвичайно складно відтворити.

Всі обговорювані сценарії MFA вимагають значних ресурсів пам'яті для статистичного аналізу вхідних даних і зберігання біометричних зразків, навіть якщо використовуються різні методи оптимізації.

Тому дуже перспективним напрямком розвитку MFA є область нейронних мереж і великих даних [40]. Тут багато успішних додатків були відомі суспільству вже більше десяти років. Приклади можна знайти в [41], де розглядаються звичайні фактори, такі як райдужна оболонка, сітківка, відбитки пальців і т. д. Використання нейронних мереж для біометрії наступного покоління - найбільш ймовірний спосіб продовжити роботу через високий рівень складності аналізу в нині.

Висновки

1. Був розглянутий підхід заснований на використанні поліномів Лагранжа для поділу секрету.

2. Запропонована зворотна методологія, заснована на поліномі Лагранжа та нове рішення MFA.

3. Запропонований вдосконалений метод оцінки рівня безпеки абонентського з’єднання.

4. Розглянуті перспективи на майбутнє.

РОЗДІЛ 5

РОЗРОБЛЕННЯ СТАРТАП-ПРОЄКТУ

У цьому розділі за темою дисертаційної роботи проводиться аналіз стартап-проекту, щоб визначити принципові можливості його впровадження та способи реалізації цього впровадження.

5.1 Опис ідеї проекту

Проаналізуємо та представляємо у вигляді таблиці зміст ідеї стартап-проекту, напрями застосування та основні переваги, які може отримати користувач продукту. Ці характеристики стартап-проекту зображено в таблиці 5.1.

Таблиця 5.1

Опис ідеї стартап-проекту

Зміст ідеї	*Напрямки застосування*	*Вигоди для користувача*
Запропонувати гнучке, ефективне та масштабоване рішення для підвищення рівня безпеки абонентського з'єднання при організації віддаленого доступу за рахунок багатофакторної автентифікації.	Застосування у повсякденному житті.	Захист персональної інформації та безпека користувачів та операторів.
	Системи віддаленого доступу, що передбачають наявність захищених ресурсів.	Можливість швидко отримати доступ до приватної системи.
	Застосування у промисловості.	Управління великою кількістю датчиків для розпізнавання людини.

5.2 Технологічний аудит ідеї проекту

У таблиці 5.2 оцінено можливість технологічної реалізації ідеї стартапу та показано технології, які можна застосувати для реалізації проекту.

Таблиця 5.2

Технологічна здійсненність ідеї проекту

№ п/п	*Ідея проекту*	*Технології її реалізації*	*Наявність технологій*	*Доступність технологій*
1	Інтеграція рішень безпеки для систем віддаленого доступу в рамках різних проектів і компаній, що працюють з абонентським з'єднанням.	Програмне забезпечення та хмарні технології застосовані на вузлах мережі	Так	Дані технології доступні
2		Спеціалізоване обладнання для використання MFA.	Ні	Можливо розробити додаткове обладнання за наявності бюджету.

5.3 Аналіз можливостей ринку для запуску проекту

У таблиці 5.3 показано попередню характеристику потенційного ринку стартап-проекту.

Таблиця 5.3

Попередня характеристика потенційного ринку стартапу.

№ п/п	Показники ринку (найменування)	*Характеристика*
1	Кількість головних гравців, од	2
2	Загальний обсяг продаж, грн/ум.од	600000
6	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу (вказати характер обмежень)	Висока точність розпізнавання, невибагливість до ресурсів, швидкодія
5	Специфічні вимоги до стандартизації та сертифікації	GDRP
6	Середня норма рентабельності в галузі (або по ринку), %	53

У таблиці 5.4 показано характеристику потенційних клієнтів стартап-проекту.

Таблиця 5.4

Характеристика потенційних клієнтів стартап-проекту.

№ п/п	*Потреба, що формує ринок*	*Цільова аудиторія (цільові сегменти ринку)*	*Відмінності поведінки потенційних цільових груп клієнтів*	*Вимоги споживачів до товару*
1	Довершення політик безпеки при розгортанні технічних систем	Компанії, які мають технічну складову	Необхідний рівень безпеки відповідно до типу компанії	Результат повинен відповідати найвищим стандартам безпеки актуальним відповідним загрозам та вразливостям які змінюються з кожним днем
2	Відповідальність, збитки та наслідки у випадку вразливості електронних систем	Компанії, які працюють з персональними даними та іншими джерелами цінної інформації, або контролюють електронні системи які несуть техногенну загрозу	Кожна група має компаній має власні вимоги до технічного забезпечення та політик і засобів безпеки відповідно	Забезпечення безпеки в залежності від потреб споживача

У табл. 5.5 наведено основні загрози реалізації стартап-проекту.

Таблиця 5.5

Фактори загроз

№ п/п	*Фактор*	*Зміст загрози*	*Можлива реакція компанії*
1	Конкуренція	На сьогоднішній день існує велика кількість засобів забезпечення безпеки	Реалізація послуг на найвищому рівні та на обладнанні провідних вендорів для надання максимально можливих та гнучких послуг відповідно до потреби клієнта
2	Швидка зміна ринку та технологій	Складність постійного надання актуальних послуг та відповідати всім тенденціям ринку.	Інвестиції в сертифікацію співробітників, моніторинг сучасних рішень від вендорів, які враховують потреби так званого «завтрашнього дня»

У табл.5.6 наведено основні можливості під час реалізації стартап-проекту.

Таблиця 5.6

Основні можливості

№ п/п	*Фактор*	*Зміст можливості*	*Можлива реакція компанії*
1	З’являються нові загрози інформаційної безпеки	Зростає потреба користувачів в надійному способі попередити подібні загрози	Розширення клієнтської бази, маркетингові дії
2	Мобільність набирає велику популярність	Зростає потреба користувачів знаходитись на великій відстані від головного офісу	Збільшення масштабів розвитку

У таблиці 5.7 наведено особливості та вплив конкурентного середовища на впровадження проекту.

Таблиця 5.7

Аналіз конкуренції

Особливості конкурентного середовища	*Прояв даної характеристика*	*Вплив на діяльність підприємства (планові дії компанії для забезпечення конкурентоспроможності)*
1. Чиста конкуренція	Застосування вже існуючих технологій	На високому рівні проводиться стандартизація.
2. Локальна конкуренція	Відсутність єдиного постачальника послуг	Індивідуальний підхід до кожної локальної ділянки
3. Регіональна конкуренція	Немає	Немає
4. Товарно-видова конкуренція	Використання стандартизованих технологій	Застосування загальновживаних апаратних та програмних засобів, за необхідності
5.Цінова конкуренція	Використання високовартісних спеціалізованих комплексів	Використання гнучких універсальних програмних засобів для компенсації апаратної частини
6. Марочна конкуренція	Значна увага приділяється бренду, що розробив продукт	Кобрендінг

У табл. 5.8 наведено та обґрунтовано фактори конкурентоспроможності.

Таблиця 5.8

Обґрунтування факторів конкурентоспроможності

№ п/п	*Фактор конкурентоспроможності*	*Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)*
1	Іноваційність	Продукт представляє реалізацію багаторівнева автентифікація для встановлення безпечного зв'язку між користувачем (клієнтом) і віддаленим сервером.
2	Конфіденційність	Продукт має стійкість проти відомих атак, дослідження потенційних атак, шаблон захисту.
3	Точність	Продукт має високу точність автентифікації, яка може бути порівняна з системами більш високого класу
4	Інтеграція	Продукт має доступний рівень прозорості, що надається постачальниками обладнання і програмного забезпечення.

За визначеними факторами конкурентоспроможності проведемо аналіз сильних та слабких сторін стартап-проекту. Результати даного аналізу зображено в таблиці 5.9.

Таблиця 5.9

Порівняльний аналіз сильних та слабких сторін системи «BioM»

№ п/п	*Фактор конкуренто-спроможності*	*Бали 1-20*	*Рейтинг товарів-конкурентів у порівнянні з BioM*						
			–3	*–2*	*–1*	*0*	*+1*	*+2*	*+3*
1	Іноваційність	16					+		
2	Конфіденційність	18		+					
3	Точність	14						+	
4	Інтеграція	14				+			

Тепер проведемо SWOT-аналіз на основі виділених загроз і можливостей, та сильних і слабких сторін проекту. SWOT-матриця зображено в таблиці 5.10.

Таблиця 5.10

SWOT-аналіз стартап-проекту

Сильні сторони: іноваційність, конфіденційність, точність, інтеграція, зручність використання.	Слабкі сторони: потреба в залученні висококваліфікованих кадрів, немає належного досвіду у веденні бізнесу.
Можливості: Кобрендінг.	Загрози: конкуренція швидко зростає на ринку.

5.4. Розроблення ринкової стратегії проекту

Обгрунтування вибору цільових груп потенціійних споживачів показано в табл. 5.11.

Таблиця 5.11

Вибір цільових груп потенційних споживачів

№ п/п	*Загальний профіль цільової групи*	*Готовність сприйняття продукту споживачами*	*Орієнтовний попит цільової групи (сегменту)*	*Напруженість конкуренції в сегменті*	*Складність входу у сегмент*
1	Компанії з технічною інфраструктурою, з високим рівнем безпеки	Висока	Високий	Середня	Середня
2	Системи віддаленого доступу в різних галузях та напрямках які на сьогодні широко розповсюджені	Середня	Середній	Середня	Низька

Визначення базової стратегії розвитку наведено у табл. 5.12.

Таблиця 5.12

Визначення базової стратегії розвитку

№ п/п	*Обрана альтернатива розвитку проекту*	*Стратегія охоплення ринку*	*Основні конкурентоспроможні позиції згідно з обраною альтернативою*	*Базова стратегія розвитку**
1	Дистриб'юція окремих елементів	Впровадження нового стандарту якості та клієнтоорієнтованості	Залучення ключових гравців у сфері телекомунікаційних систем	Стратегія диференціації
2	Бюджетність проекту в порівнянні з іншими гравцями ринку	Інвестиція в кваліфіковані кадри	Використання унікальних, інноваційних, передових рішень для досягнення лідерських позицій	Стратегія лідерства по якості послуг та рівню обслуговування

Визначення основної стратегії конкурентної поведінки показано в табл. 5.13.

Таблиця 5.13

Визначення базової стратегії конкурентної поведінки

№ п/п	*Чи є проект унікальним на ринку?*	*Чи необхідно буде компанії шукати нових споживачів, чи опрацьовувати існуючих у конкурентів?*	*Чи необхідно компанії копіювати основні характеристики товару конкурента?*	*Стратегія конкурентної поведінки**
1	Так	Опрацьовувати існуючих та шукати нових	Немає необхідності	Стратегія інноваційної конкуренції

Визначення стратегії позиціонування показано в табл. 5.14.

Таблиця 5.14

Визначення стратегії позиціонування

№ п/п	Вимоги цільової аудиторії до товару	Основна стратегія розвитку	Основні конкурентоспроможні позиції стартаппроекту	Визначення асоціацій, які сформують комплексну позицію стартап-проекту (три основних)
1	Належна висока якість послуг	Стратегія диференціації	Новизна, гарант якості, точність дослідження	Якість, точність, надійність
2	Раціональні витрати	Стратегія лідерства по витратах	Гнучкість запропонованого рішення	Універсальність, інноваційність, надійність

5.5. Розроблення маркетингової програми стартап-проекту

Основні переваги концепції потенційного товару показано в табл. 5.15.

Таблиця 5.15

Визначення основних переваг концепції потенційного товару

№ п/п	*Потреба*	*Вигода, яку пропонує товар*	*Основні переваги перед конкурентами (існуючі або потенційні)*
1	Якість	Належна висока якість, надійність	Масштабованість, гнучкість, якість
2	Раціональна вартість	Оптимальне використання коштів, максимальна якість обладнання від провідних вендорів, максимальний рівень кваліфікації спеціалістів в залежності від вартості та складності проекту	Раціоналізація витрат відповідно до розміру бюджету замовника

Виявлено три рівні моделі товару. Зміст та складові рівнів товару показано в табл. 5.16.

Таблиця 5.16

Опис трьох рівнів моделі товару

<table>
<tr><td>Рівні товару</td><td colspan="3">Зміст та складові</td></tr>
<tr><td>I. Товар за задумом</td><td colspan="3">Якісний товар та послуги, стандартизована якість послуг та обладнання</td></tr>
<tr><td rowspan="5">II. Товар у реальному виконанні</td><td>Властивості/характеристики</td><td>М/Нм</td><td>Вр/Тх /Тл/Е/Ор</td></tr>
<tr><td>1)Вартість обслуговування,
2)Кількість комплектів обладнання
3)Строк безвідмовної експлуатації 4)Технологічна собівартість товару</td><td>1) М
2) М
3) М
4) М</td><td>1)Е
2) Пр
3)Нд
4)Тх</td></tr>
<tr><td colspan="3">Якість: міжнародні стандарти, постійне обслуговування та підтримка обладнання</td></tr>
<tr><td colspan="3">Постачання, розрахунки та інтеграція під конкретні системи</td></tr>
<tr><td colspan="3">Марка: Системи безпеки</td></tr>
<tr><td rowspan="2">III. Товар із підкріпленням</td><td colspan="3">До продажу – обладнання та встановлення</td></tr>
<tr><td colspan="3">Після продажу – аудит та вдосконалення застарілих елементів та систем в цілому в залежності від актуальних вимог та потреб</td></tr>
</table>

Потенційний товар буде захищено від копіювання завдяки: товарна марка та унікальні рішення, які не мають аналогів на ринку та відрізняються між собою оскільки кожне з рішень є глибоко індивідуальним в залежності від потреб замовника, що необхідно для забезпечення найвищих та актуальних на майбутнє стандартів безпеки.

Визначення цінової політики на послугу показано в табл. 5.17.

Таблиця 5.17

Визначення меж встановлення ціни

№ п/п	Цінова політика товарів-замінників	Цінова політика на товарианалоги	Рівень купівельної спроможності цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу
1	40000 у.о./од. (стандартні системи безпеки)	-	Дуже високий	Н.1000 у.о. – В.100000 у.о. (Товар) Н.1000 у.о. – 94 В.100000 у.о. (Послуга)

Створення системи збуту послуги вказано у табл. 5.18.

Таблиця 5.18

Створення системи збуту

№ п/п	*Закупівельна поведінка цільових клієнтів*	*Функції збуту, що повинен забезпечувати постачальник товару*	*Глибина каналу збуту*	*Оптимальна система збуту*
1	Орієнтована на максимальний рівень безпеки в системах різного роду	Поставки якісного обладнання та інноваційних рішень	Значна	Контрактна система

Концепції маркетингових комунікацій показано в табл. 5.19.

Таблиця 5.19

Концепція маркетингових комунікацій

№ п/п	*Специфіка поведінки цільових клієнтів*	*Канали комунікацій цільових клієнтів*	*Основні методи позиціонування*	*Завдання рекламного звернення*	*Концепція рекламного звернення*
1	Зацікавленість якісному та якісному продукті з раціональним використанням ресурсів	Мережеві ресурси	Гарантія якості та стандартизація, сервісна політика	Привернути увагу до покращень, пов'язаних із зростаючою потребою в захисті	Позиціонування безпеки як основи для побудови надійних рішень та іміджу компанії
2	Зацікавленість у великих об'ємах продукції із дотриманням умов якості	Мережні ресурси	Глибина каналу постачальників, гарант якості	Привернути увагу до переваг над іншими гравцями ринку	Позиціонування як активного та інноваційного гравця ринку 95 на фоні конкурентів

Висновки

1. Результат дослідження, проведеного у рамках дисертаційної роботи (а саме запропонований підхід щодо підвищення рівня безпеки абонентского з'єднання) може стати основою для успішного стартап-проекту;

2. Для стартап-проекту за темою магістерської дисертації визначено характеристика потенційного ринку, фактори загроз, основні можливості, а також проведений аналіз конкурентоспроможності;

3. За визначеними факторами конкурентоспроможності проведемо аналіз сильних та слабких сторін стартап-проекту.

4. Проведено аналіз ринкових можливостей запуску стартап-проекту, у результаті якого визначено, що проект може стати привабливим для ринку завдяки своїй іноваційності, конфіденційності, точності, інтеграції та зручність використання.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

У роботі на здобуття освітнього ступеня Магістра було досліджено вдосконалений метод оцінки рівня безпеки абонентського з'єднання при організації віддаленого доступу.

У процесі дослідження були виявлені проблеми захисту інформації при організації віддаленого доступу та був проведений огляд можливих заходів для забезпечення заданого рівня безпеки. Так як автентифікація залишається основним захистом від незаконного доступу до пристрою чи будь-якого іншого додатка, у своїй роботі я вирішила покращити рівень безпеки абонентського з'єднання за рахунок використання багатофакторної автентифікації для взаємодії між людьми, забезпечуючи швидку, зручну і надійну автентифікацію при доступі до послуги.

Підводячи підсумок, можна сказати, що біометричні технології - це важливий напрямок, що визначається ринком мобільних пристроїв. Вважається, що сильний поштовх до використання біометрії в багатьох сферах життя неминучий, оскільки більшість флагманських пристроїв вже оснащені сканером відбитків пальців і технологією розпізнавання осіб на додаток до стандартних PIN-кодів.

Ця робота надала систематичний огляд сучасного стану як технічних питань, так і питань зручності використання, а також основних проблем в існуючих в даний час системах MFA. У цьому дослідженні було обговорено еволюцію автентифікації від однофакторних систем до багатофакторних.

В першу чергу було зосереджено увагу на факторах MFA, складаючих сучасний стан, можливих майбутніх напрямків, що відповідають проблемам і перспективним рішенням. Було також запропонували рішення MFA, засноване на зворотному поліномі Лагранжа, як розширення схеми спільного

використання секретів Шаміра, яка охоплює випадки автентифікації користувача, навіть якщо деякі з факторів не збігаються або відсутні. Це також допомагає кваліфікувати відсутні чинники, не розкриваючи конфіденційні дані перевіряючої сторони.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Введение в технологии удаленного доступа Microsoft и их краткий обзор / [Електронний ресурс] – Режим доступу: http://www.oszone.net/4086/Microsoft_RemoteAccess.

2. Терминальный доступ: понятие, преимущества, недостатки и особенности работы данной системы / [Електронний ресурс] - Режим доступу: http://www.shindler.ru/content/terminalnyi-dostup-ponyatie-preimushchestva-nedostatki-i-osobennosti-raboty-dannoi-sistemy.

3. Методы удаленного доступа / [Електронний ресурс] – Режим доступу: https://studopedia.su/1_31452_metodi-udalennogo-dostupa.html.

4. Nathan J. Muller. Remote Access Techniques / [Електронний ресурс] – Режим доступу: http://www.ittoday.info/AIMS/DCM/51-20-52.PDF.

5. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа // Наука и Техника, ст. 160-190, (2004).

6. Christina M. Bird, Ph.D, CISSP.: An introduction to secure remote access, ст. 17-67, (2000).

7. Олифер В.Г., Олифер Н.А.: Компьютерные сети, ст. 32-38, (2009).

8. Ибе О.: Компьютерные сети и службы удаленного доступа, ст. 344, (2014).

9. Навчальний посібник для студентів спеціальності 151 «Автоматизація та комп’ютерно-інтегровані технології» / [Електронний ресурс] – Режим доступу: http://divovo.in.ua/navchalenij-posibnik-dlya-studentiv-specialenosti-151-avtomati.html?page=10.

10. Aboba D., Mitton B. Zorn G.: RADIUS and IPv6, RFC 3162, (2001).

11. VNI Cisco Global Mobile Data Traffic Forecast 2016–2021 /

[Електронний ресурс]. – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-indexvni/complete-white-paper-c11-481360.pdf.

12. Lamport, L.: Password authentication with insecure communication. Commun. ACM 1981, 24, 770–772.

13. Benarous, L.; Kadri, B.; Bouridane, A.: A Survey on Cyber Security Evolution and Threats: Biometric Authentication Solutions. In Biometric Security and Privacy; Springer: Berlin, Germany, ст. 371–411, (2017).

14. Balloon, A.M.: From Wax Seals to Hypertext: Electronic Signatures, Contract Formation, and a New Model for Consumer Protection in Internet Transactions. Emory Law J., ст. 50, 905, (2001).

15. Heartfield, R.; Loukas, G.: A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. ACM Comput. Surv. (CSUR), ст. 48, 37, (2016).

16. Gunson, N.; Marshall, D.; Morton, H.; Jack, M. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking, ст. 30, 208–220, (2011).

17. National Research Council; Whither Biometrics Committee. Biometric Recognition: Challenges and Opportunities; National Academies Press: Washington, DC, USA, (2010).

18. Aloul, F.; Zahidi, S.; El-Hajj, W.: Two factor authentication using mobile phones. In Proceedings of the International Conference on Computer Systems and Applications, Rabat, Morocco, ст. 641–644, (2009).

19. De Cristofaro, E.; Du, H.; Freudiger, J.; Norcie, G.: A comparative usability study of two-factor authentication. arXiv 2013, arXiv:1309.5344.

20. Ratha, N.K.; Connell, J.H.; Bolle, R.M.: Enhancing security and privacy

in biometrics-based authentication systems. IBM Syst. J., ст. 40, 614–634, (2001).

21. Schroff, F.; Kalenichenko, D.; Philbin, J. Facenet: A unified embedding for face recognition and clustering. In Proceedings of the Conference on Computer Vision and Pattern Recognition, Boston, MA, USA, ст. 815–823, (2015).

22. Feng, T.; Liu, Z.; Kwon, K.A.; Shi, W.; Carbunar, B.; Jiang, Y.; Nguyen, N.: Continuous mobile authentication using touchscreen gestures. In Proceedings of the Technologies for Homeland Security (HST) Conference, Waltham, MA, USA, ст. 451–456, (2012).

23. Kun, A.L.; Royer, T.; Leone, A. Using tap sequences to authenticate drivers. In Proceedings of the 5th International Conference on Automotive User Interfaces and Interactive Vehicular Applications, Eindhoven, ст. 228–231, (2013).

24. Busold, C.; Taha, A.; Wachsmann, C.; Dmitrienko, A.; Seudié, H.; Sobhani, M.; Sadeghi, A.R.: Smart keys for cyber-cars: Secure smartphone-based NFC-enabled car immobilizer. In Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy, ст. 233–242, (2013).

25. Thullier, F.; Bouchard, B.; Menelas, B.A.J.: A Text-Independent Speaker Authentication System for Mobile Devices. Cryptography, ст. 1, 16, (2017).

26. Ahonen, T.; Hadid, A.; Pietikainen, M.: Face description with local binary patterns: Application to face recognition. IEEE Trans. Pattern Anal. Mach. Intell., ст. 28, 2037–2041, (2006).

27. Bhattacharyya, D.; Ranjan, R.; Alisherov, F.; Choi, M. Biometric authentication: A review. Int. J. u- e-Serv. Sci. Technol., ст. 2, 13–28, (2009).

28. Zheng, G.; Wang, C.J.; Boult, T.E.: Application of projective invariants in hand geometry biometrics. IEEE Trans. Inf. Forensics Secur., 2, ст. 758–768, (2007).

29. Kumar, A.; Hanmandlu, M.; Madasu, V.K.; Lovell, B.C. Biometric authentication based on infrared thermal hand vein patterns. In Proceedings of the Digital Image Computing: Techniques and Applications (DICTA'09), Melbourne, VIC, Australia, ст. 331–338, (2009).

30. Chen, B.; Chandran, V. Biometric template security using higher order spectra. In Proceedings of the International Conference on Acoustics Speech and Signal Processing (ICASSP), Dallas, TX, USA, ст. 1730–1733, (2010).

31. Gomez-Barrero, M.; Rathgeb, C.; Galbally, J.; Busch, C.; Fierrez, J. Unlinkable and irreversible biometric template protection based on bloom filters. Inf. Sci., ст. 370, 18–32, (2016).

32. . Wayman, J.; Jain, A.; Maltoni, D.; Maio, D.: An introduction to biometric authentication systems. Biom. Syst., ст. 1–20, (2005).

33. Lichtman, M.; Jover, R.P.; Labib, M.; Rao, R.; Marojevic, V.; Reed, J.H.: LTE/LTE-A jamming, spoofing, and sniffing: Threat assessment and mitigation. IEEE Commun. Mag. ст, 54, 54–61.

34. Ratha, N.; Bolle, R.: Automatic Fingerprint Recognition Systems; Springer: Berlin, Germany, (2007).

35. . Golfarelli, M.; Maio, D.; Malton, D. On the error-reject trade-off in biometric verification systems. IEEE Trans. Pattern Anal. Mach. Intell., ст. 19, 786–796, (1997).

36. Schneier, B.: Two-factor authentication: Too little, too late. Commun, ст. 48, 136, (2005).

37. Kaya, K.; Selçuk, A.A.: Threshold cryptography based on Asmuth–Bloom

secret sharing. Inf. Sci., ст. 177, 4148–4160, (2007).

38. Thakkar, D. False Acceptance Rate (FAR) and False Recognition Rate (FRR) in Biometrics, / [Електронний ресурс] – Режим доступу:https://www.bayometric.com/false-acceptance-rate-far-false recognition-rate-frr/.

39. Castanedo, F.: A review of data fusion techniques. Sci. World J., ст. 1–19, (2013).

40. Berry, P. Biometrics and Artificial Neural Networks: How Big Data Collection Works in Your Favor, / [Електронний ресурс] – Режим доступу:http://chicagopolicyreview.org/2014/03/04/biometrics-and-artificial-neural-networkshow-big-data-collection-works-in-your-favor/.

41. Sadikoglu, F.; Uzelaltinbulat, S.: Biometric Retina Identification Based on Neural Network, ст, 26–33, (2016).